uTRUSTit – Usable Trust in the Internet of Things
Project Reference: 258360
FP7-ICT (Area: ICT-2009-1.4 Trustworthy ICT)
Project Duration: 1 Sep 2010 – 31 August 2013

D.7.2 Legal Requirements for the Office and the Home Scenario

[K.U.Leuven]

FINAL

Authors:
Jos Dumortier (K.U.Leuven)
Niels Vandezande (K.U.Leuven)

Version: 1.0
Date: 04/09/2011
Dissemination level: (PU, PP, RE, CO): PU

Project Co-Funded by the European Commission within the 7th Framework Programme

Abstract:

The Internet of Things (IoT) will connect a large number of communication and information systems. These systems will be part of everyday life in the same way mobile phones have become part of our lives. The information security properties of the IoT are often difficult to understand for its users, because they are hidden in pervasive systems and small devices manufactured by a large number of vendors. Trustworthiness, security functions and privacy implications are vast, and must be assessable to users and consumers.

The main focus of the uTRUSTit project lies in its objective to integrate the user directly in the trust chain, guaranteeing transparency in the underlying security and reliability properties of the IoT. The results of uTRUSTit enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgments on the trustworthiness of such systems. Further, uTRUSTit's design guidelines on trust help the industry to implement the trust-feedback toolkit developed by uTRUSTit in a secure, usable and accessible way.

This report will further develop the general legal requirements conceived under Deliverable 7.1 (Legal Requirements for Trust in the IoT) and apply them to the Office and Home Scenario, as developed under Deliverable 2.2 (Definition of User Scenarios). Also the needs of the personas, as developed under Deliverable 2.1 (Personas) will be analyzed from a legal point of view. From this analysis, legal requirements will be developed to ensure that the prototypes that will be built to implement the solutions developed in the scenarios are fully legally compliant. Amongst others, it will be indicated whether the information that is shared in the chain of devices should be considered as personal data that is subject to the relevant privacy and data protection legislation, and the legal obligations that follow from this qualification.

Table of Contents

1. INTRODUCTION 5

1.1 Background 5
1.2 Scope of this Deliverable 5

2. LEGAL ANALYSIS OF PERSONAS 6

2.1 Anna Janssen 6
2.2 David Clasen 7
2.3 Paul Clasen 8
2.4 Fredrik Clasen 8
2.5 Sara Moser 9
2.6 Summary 9

3. LEGAL ANALYSIS OF SCENARIOS 11

3.1 Smart Home Scenario 11
3.2 Smart Office Scenario 12
3.3 Summary 13

4. DEVELOPMENT OF LEGAL REQUIREMENTS 14

4.1 General data protection requirements 14
4.1.1 Data protection and privacy at home 14
4.1.2 Data protection and privacy at the office 16
4.2 Informed consent requirements 20
4.2.1 Effectiveness of consent 21
4.2.2 Capacity to consent 22
4.3 Health monitor requirements 24
4.3.1 Adaptability of the health monitoring system 24
4.3.2 Processing of health data 26
4.4 Electronic payments requirements 27
4.4.1 Electronic payment transactions 28
4.4.2 Trustworthiness of electronic information 31
4.5 Security and access management requirements 32
4.5.1 Confidentiality requirements 33
4.5.2 Security requirements 34
4.6 Technology requirements 36
4.6.1 General privacy concerns 37
4.6.2 Geolocation applications 38
4.7 Intellectual property rights requirements 39
4.7.1 Possibility of copyright infringements 40
4.7.2 Producer's liability for copyright infringements 41

5. CONSOLIDATION OF LEGAL REQUIREMENTS 43

6. SUMMARY 48

7. REFERENCES 49

7.1 Legislative sources 49
7.2 Case law 50
7.3 Legal literature 50

List of acronyms

ATM	Automated Teller Machine
ECHR	European Court of Human Rights
ECJ	European Court of Justice
EDI	Electronic Data Interchange
EDPS	European Data Protection Supervisor
GPS	Global Positioning System
IoT	Internet of Things
NFC	Near Field Communication
PET	Privacy-Enhancing Technologies
RFID	Radio -Frequency Identification
UN	United Nations

1. Introduction

1.1 Background

The work under Work Package 7 establishes a set of clear legal requirements for trust in the IoT and takes into consideration all relevant legislation, amongst which legislation relating to privacy and the protection of personal data. It comprises the legal evaluation of the prototypes envisioned in the scenarios in order to ensure legal compliance. Furthermore, this work package is to prove whether uTRUSTit's activities and in particular its results are in accordance with Europe's ethical values and standards. The ethical aspect of this work package was finalized under Deliverable 7.4 (Ethics Manual).

1.2 Scope of this Deliverable

This report will present the final results of the research performed in task 7.2 (Legal Requirements for the Office and the Home Scenario). It will further develop the general data protection requirements conceived under Deliverable 7.1 (Legal Requirements for Trust in the IoT), with specific attention for application of these requirements to the Office and Home Scenario, as developed under Deliverable 2.2 (Definition of User Scenarios). As the Office and Home Scenario were developed keeping in mind the Personas developed under Deliverable 2.1 (Personas), this report will analyze the personas and their specific needs from a legal point of view.

This document will therefore specifically look at the legal requirements for the Smart Home and the Smart Office scenario and how the user can trust the devices. Regarding these scenarios, the general legal privacy policy framework stipulating legal requirements formulated in Task 7.1 will be applied so that the prototype can be designed with a clear set of legal requirements in mind. This report will, amongst others, analyze and determine whether information shared in the chain of devices is personal data that is subject to the relevant privacy and data protection legislation.

This report will furthermore investigate what information, if any, may be shared on online communities and ascertaining in what circumstances the consent of the user is required. Due attention will be given to processing of what may be considered potentially sensitive data such as information relating to the health of the user and which information may be processed by devices in the network of IoT in a smart home scenario.

2. Legal Analysis of Personas

The uTRUSTit project aims to create guidelines, systems and interfaces that allow anyone, regardless of their ability, to determine the level of security and their own trust in the devices around them [UTRUSTIT 2011a]. In order to develop usable scenarios and technology, extensive testing by a representative user base is imperative. However, compiling and having continuous access to such user base is rather costly and time-consuming. As a result, developers often focus on the idea of the generic user, exposing the project to the risk of failing to take into account the specific needs of particular persons from different demographic backgrounds. Therefore, it was decided that the uTRUSTit project would make use of *personas*, hypothetical archetypical users from different demographic backgrounds that have clearly defined goals and needs.

The personas to be used as targeted users in the uTRUSTit project were first developed at the Personas Workshop, held in Budapest on 1 December 2010 [UTRUSTIT 2010]. The definitive incarnations of the personas were further developed under Deliverable 2.1 – Personas [UTRUSTIT 2011a]. By including personas with certain disabilities – such as dyslexia and vision impairment – it is ensured that these demographics are represented and taken into account in the development of the uTRUSTit solutions.

The development of the specific goals and needs of the personas, as well as of their demographic background, does not provide insights that are only useful for the technical developments within the project. It can also serve as a starting point for the development of the legal requirements to which the final prototype will need to respond. With the personas in mind, these legal requirements can be developed early on in the project, to ensure that they are already taken into account during the technical development process. Such will avoid legal incompliance and potential major revisions in the later stages of the project.

Therefore, the personas will be analyzed in order to extract the legal implications from their specific situations, goals and needs. Such legal implications will later on in the present deliverable form the basis for the development of the legal requirements.

2.1 Anna Janssen

As part of her job as a help desk assistant in an online shop, Anna will process all kinds of data, some of which – such as names, addresses and payment details – are to be considered as personal data in the sense of the European legal framework on data protection. Therefore, it is important to determine the capacity in which she performs such personal data processing. As she processes this data in the execution of her obligations under her agreement of employment with her employer, it will be the employer that acts as the data controller of such processing. As she is a direct employee of her employer, and not an external party contracted for this processing, she will not be considered as a processor. As a result, Anna will have to comply with the means and purposes on the processing of personal data determined by her employer. Here, one will have to assess how the assistive technologies used by Anna fit into the requirements set to the processing of personal data. For instance, does the screen reader log the data it reads to Anna? If so, it will be important to know how such logs are stored and who can access them.

Anna's wishes to be reminded when certain items run out of stock, to be able to look for items she misplaced and to manage all connected objects in her household would require the possibility to track such items and objects. While existing technologies – such as Radio-Frequency Identification (RFID) – already allow for such application, these technologies are often subject to a number of legal concerns. The development of specific requirements to which the use of such technologies in this context needs to respond is therefore imperative.

Last, some of Anna's wishes would imply the processing of personal data, be it for personal and household use. Examples here are her wishes for an online Laundromat booking application, to coordinate all of her family's appointments and to monitor her daughter's online activities. While further analysis could indicate that such personal data processing would fall under the household exception as analyzed under Chapter 4.2.3 Application of the household exception of Deliverable 7.1 Legal Requirements for Trust in the IoT [UTRUSTIT 2011b], one should still refer to the general provisions regarding privacy, as found in article 8 of the European Convention on Human Rights (ECHR), amongst others.[1]

2.2 David Clasen

David's stance on manuals as being only understandable by experts may also reflect his position with regards to consent forms. As analyzed under Chapter 4.2.6 How to obtain the data subject's consent? of Deliverable 7.1 Legal Requirements for Trust in the IoT [UTRUSTIT 2011b], a consent form needs to contain rather elaborate information regarding the precise workings of the processing of personal data, its means and purposes, its actors and their specific roles, etc. in order to provide the data subject with the information he needs to provide his fully informed consent. However, as such elaborate consent forms more often than not result in an almost unintelligible text, they are not always fully read by data subjects. David's stance on manuals could be an indication that David is one of the many people that, for instance, just click the "click-to-accept"-button on a website, resulting in the provision of consent without understanding to what they consented. For David, one could therefore refer to the layered consent form as analyzed under Deliverable 7.1. User-friendliness, both with regards to technical manuals and documents with legal consequences such as consent forms, should prevail in order to make technology more accessible and trustworthy towards people with an attitude of general mistrust in technology that they do not understand.

David's more successful encounter with technology comes in the form of a health monitoring system set up in the home of his father, Paul. Apart from monitoring Paul's general condition, this system also includes a warning function in case of emergency – for instance when Paul falls – and a function to monitor Paul's medical cabinet. The system also allows David to remotely grant access rights to Paul's home, in case a healthcare organization needs to make an unscheduled emergency visit. While such system certainly aids in the caretaking of the elderly that want to retain certain independence, it also raises a number of legal questions. For one, as Paul is the one who is being monitored, he will have to provide his consent in all of this. With the elderly, this raises the additional question regarding their capacity to provide consent and who could possibly grant such consent on their behalf. Second, one will need to assess how intrusive such system can be. Should it be allowed to monitor continuously, or should there be an option for the person being monitored to shut down the system when he wants to? Last, it should be noted that this system processes data regarding the medical condition of a natural person, which falls under the scope of sensitive data according to the European legal framework on data protection. One will therefore have to establish a clear list of requirements to which the working of such health monitoring system should respond.

While online shops are playing an ever-growing role in the world's economy, there are still many people that – like David – do not trust the online payments associated with such transactions. One of his fears is whether his credit card data is handled securely. While this raises mostly technical questions, it also has a few legal aspects, for instance relating to technologies of which the use is already embedded in law, such as the electronic signature. Further trust in online payments could be generated by ensuring that all statements received in the process – be it in the form of actual electronic documents, such as an electronic invoice, or in the form of simple user interface feedback – are true and reliable. Here, one could refer to the legal value of electronic information, whereby the value and

[1] Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950.

general trustworthiness of such electronic information could be established by ensuring the authenticity and integrity of such information.

2.3 Paul Clasen

Paul has already been referred to in the analysis of his son, David Clasen. Paul is the subject of the health monitoring system set up by his son and also accessible to a private healthcare organization that makes regular visits and can also intervene in case of emergency.

The main legal issue that can be derived from Paul's situation refers to his consent. He is the subject of a health monitoring system – which also allows his son to remotely grant access rights to the house – his grandson has remote access to his computer, his mobile phone is essentially used to track his whereabouts, etc. While he appreciates certain aspects of this elaborate system, such as the reminders, his unfamiliarity with modern technology makes it difficult for him to accept this system. He has also indicated that he finds certain elements too intrusive and asked his grandson to help him disable these elements. However, he has to tolerate this system as it allows him to maintain certain independence and to keep living in his own home. Without such system, he would have to move in with his family or possibly even relocate to a more suited facility such as a retirement home.

The tradeoff between retaining certain independence while under surveillance or losing all independence raises the question as to whether this can still be considered as being consent given out of the data subject's own free will, as required under existing data protection legislation. As already hinted at, one may also wonder whether Paul – given his early-stage dementia – is still legally capable of providing his own consent. Additionally, one should also assess in how far Paul retains certain control over the processing of his personal data through the use of such system. Can he opt-out of certain features he finds too intrusive? Therefore, legal requirements will have to be drafted to ensure that legally valid consent can be provided in the use of such health monitoring system. These requirements also need to keep in mind the possibility of the further deterioration of Paul's state of mind, which could make future revocation or modification of his consent – given when he was still capable thereto – impossible.

2.4 Fredrik Clasen

While David Clasen is a clear example of a person with a general mistrust against modern technology, his son, Fredrik, serves as an example of somebody who might confer too much trust onto technology. Surprisingly, the legal implications are rather similar: as Fredrik, like his father, never reads manuals and legal documents such as privacy policies, he is exposed to the risk of granting his consent without fully knowing to which he consented. This overconfidence is also reflected in his stance on passwords and security. Therefore, one could look into how technology can be used to ensure that the data subject actually read and understood the consent form before providing his consent. As forcing a user to read through such often unintelligible text would have a negative impact on his user experience, one will have to keep user-friendliness in mind here as well, especially with regards to Fredrik's dyslexia and his use of assistive technologies.

In general, his lack of care for security with regards to his personal data and his online transactions expose Fredrik to a number of other risks as well. With recent waves of data theft, hacking and other types of cybercrime, the importance of IT security is stressed once more.[2] Adequate security is already required by data protection legislation. Current developments indicate that a notification duty in case of data theft may be adopted in the near future. One will therefore have to analyze the

[2] Note, for instance, the numerous high-profile cases of data theft – notably including personal data of users of the Sony Playstation Network – by collective LulzSec in June 2011, *itpro.co.uk/634393/timeline-lulzsec-hack-attacks*.

current legal provisions – and possible future developments – with regards to data and IT security in order to establish the legal requirements hereof. As with consent, user-friendliness should be kept in mind.

Fredrik's experiments with technology could have implications regarding the warranty on these devices. Any use that does not conform with the use intended by the manufacturer of a product could result in voiding the product's warranty. Furthermore, under the European legal framework on product liability, such unintended use could lead to shared liability between the product's manufacturer and the user. As a result of such shared liability, the user will not receive full compensation for the damages caused to him by the faulty product, which he would have received if he had used the product as intended by its manufacturer.

Fredrik's wish to share media data with his friends may raise questions with regards to copyright legislation. If they share copyrighted data, they will have to ensure that such sharing falls under the scope of fair use. Legal requirements are therefore needed to ensure that such media sharing system limits its functionality to what is permitted under copyright law, for instance by limiting access to the media data to properly licensed users. As will be explained further on – in chapter 4.7.2 - Producer's liability for copyright infringements – it will also be important to establish what the media sharing system or application was intended for by its producers.

2.5 Sara Moser

Sara's wishes are mainly aimed at accessibility. She wants to be able to remotely provide access rights to her apartment and to be able to access her personal files from wherever she goes. Using collaborative tools, remote and wireless connections, location based services and cloud computing applications, security is of utmost importance to her. This accessibility also has to be dynamic. She wants to change the access rights to her apartment when necessary, to provide meeting partners temporary and limited access to certain data and to control the information that is accessible about her.

As with Fredrik, one will have to assess the current legal provisions with regards to data and IT security in order to establish the legal requirements with which such systems need to comply.

2.6 Summary

While the personas show very different goals and needs and are of different demographic backgrounds, there are a number of recurring themes when analyzing their goals and needs from a legal point of view.

First, the data protection requirements developed under D7.1 Legal Requirements for Trust in the IoT will have to be applied to the specific situations of the personas. For instance, it will have to be analyzed what the influence is of the use of assistive technologies in processing personal data as part of one's job.

Privacy related requirements should not only be aimed at professional processing of personal data. For instance, if one wants to keep track of one's family's appointments or Internet behavior. While such would occur in a household setting – thus possibly benefiting from an exception to the general obligations under European data protection legislation – one should still bear in mind general privacy provisions.

Further with regards to data protection and privacy, there are a few issues regarding consent. First, it is clear that certain data subjects do not fully read consent forms and privacy policies – be it due to mistrust of technology or out of overconfidence in technology – and are thus exposed to the risk of

providing consent without knowing to which they consented. While consent forms should provide complete information, they should also keep user-friendliness in mind. Furthermore, guarantees are needed towards their effectiveness. Another consent issue concerns elderly persons who are subjected to a health monitoring system in order to maintain a certain level of independence. Can such trade-off still be considered as freely given consent and are elderly persons with onsets of dementia still capable of providing consent?

The health monitoring system also raises questions with regards to its functionalities and its adaptability to the specific needs of users. For instance, can a location-tracking component be disabled when not needed? Also, as health data is processed in using such health monitoring system, one will have to keep in mind the requirements on processing this type of sensitive data set by the European legal framework on data protection.

Next, in order to generate more trust in online payment transactions, one will have to analyze the requirements set by specific legislation relating to transactions, such as legislation concerning e-commerce. In order to ensure that electronic information is truthful and trustworthy, one can also establish its authenticity and integrity, relating to the legal value of said information.

Another general issue concerns security and access management. Regardless of whether a certain individual cares for security or not, adequate security features are imperative for any trustworthy product when dealing with the number of interconnections and subsequent security risks posed by the IoT. Also from a legal point of view, security has become the subject of specific legal provisions, for instance with regards to the storage of personal data. Specific requirements looking at security from a legal perspective are therefore needed.

Last, one should look at the specific technologies used to implement certain of the features desired by the personas, such as the object tracking system that could potentially be realized using technologies such as RFID. This warrants specific legal requirements relating to the use of such technologies for the purposes envisioned here.

While most of the previous is aimed at formulating legal requirements with which the solutions offered to the personas will have to comply, one should also keep their intended use by the personas themselves in mind. For instance, if the intended use of a media center constitutes a breach of what can be considered as fair use under copyright law, one should ensure that such media center is designed to promote only legitimate use.

3. Legal Analysis of Scenarios

The technology to be developed within the uTRUSTit project will be demonstrated in three different settings. These settings are developed within three scenarios: the Smart Home, the Smart Office and the E-Voting scenario [UTRUSTIT 2011c]. Under the scope of this deliverable, the Smart Home and Smart Office scenario will be analyzed.

The scenarios are designed to reflect challenges for building trust with the connected elements in the IoT. Using the personas developed for use within the project, the scenarios were designed to provide solutions to the specific goals and needs of these personas. This makes the scenarios more realistic and relatable. These scenarios are presented as technology-neutral. Specific requirements for technologies to be used will be defined in a separate deliverable, D2.4 Technical Requirements for the IoT Prototype.

As with the personas, the scenarios will be analyzed from a legal point of view in order to extract the legal implications of the solutions envisioned within the uTRUSTit project. Such legal implications will later be developed into legal requirements to which the prototype will need to respond.

3.1 Smart Home Scenario

Smart home technology is a collective term for information- and communication technology (ICT) as used in houses, where the various components are communicating via a local network [UTRUSTIT 2011c]. The Smart Home scenario has been divided into three applications: Trusted Smart Home Services, Trusted Smart Home Entertainment Management and the Inventory of Things.

The Trusted Home Scenario was developed around the needs of the Paul Clasen persona, who suffers from the onsets of dementia yet wants to retain independency while under surveillance by a health monitoring system. For instance, the scenario describes the remote access management system to Paul's home and his medical cabinet. This enables his son to dynamically change access rights when needed. This corresponds to the legal implication of security and access management, as mentioned under chapter 2.6 summary of this deliverable.

The Trusted Home application also provides for medicine management and control. Apart from controlling who can access this cabinet, the cabinet can also keep track of its contents. It can notify Paul when he needs to take a pill, which pill to take, and alert Paul's attending physician to prescribe a refill. Such application would require the use of RFID technology and a secure Internet connection between the parties involved, which includes the attending physician, the pharmacist and a healthcare worker. Therefore, the legal implications of the use of these technologies for the purposes intended here will have to be analyzed. Also, as this medicine management system includes the processing of health data, one will have to bear in mind the requirements set to the processing of this type of sensitive personal data. For instance, it needs to be assessed whether the cabinet keeps track of all medication and how such tracking logs are protected. Furthermore, it will need to be clear who has access to such data and how such data is stored.

This application also includes the use of location tracking services, embedded within Paul's mobile phone or his uTRUSTit device. Such would allow his son – or in case of emergency also healthcare workers – to track Paul's movements. This raises a number of legal questions. For one, the continuous tracking of a person's whereabouts is rather invasive to the privacy of that person.[3] Adequate consent will therefore have to be provided. Sufficient access rights need to ensure that only authorized persons have access to this tracking ability and the data it collects and stores. Also, one will

[3] Note, for instance, the case in which the popular iPhone was found to store a file keeping track of every movement of its user, even if such user thought he had disabled all functions regarding geolocalization data [ALLEN 2011].

have to assess what degree of user control is needed. Should Paul be able to disable the tracking option when he wants to? Last, as with RFID, the use of Global Positioning System (GPS) technologies calls for legal requirements to which the use of such technologies in this context should respond.

The Trusted Smart Home Entertainment Management application allows visitors to bring their own music to play on the Clasen family's home media center. This media center manages all types of media owned by the family and provides for wireless streaming in all rooms. For visitors, adequate access rights management and security will be required to provide access to play music, yet while shielding of personal media, such as family photos. Apart from Wi-Fi and RFID, this system could also make use of Bluetooth and Near Field Communication (NFC), corresponding to the need for requirements for the use of such technologies in this context, as explained before. The media center also has an Internet connection, enabling the purchase of music online and the direct upload of this music to the media center. Such online transactions were also discussed under the analysis of the personas. The Smart Home Entertainment Management application also raises questions with regards to the compliance with copyright protection. For instance, if a visitor brings his own music to the Clasen family's home media center and if that music is uploaded to that media center, then a copy of the music has effectively been made. Therefore, it needs to be analyzed in how far such would correspond with fair use and how copyright infringements can be avoided.

Last, the Inventory of Things allows for one to maintain an overview on other devices in the IoT and to control what information these devices request and what is effectively transmitted. In practice, this application scans whether data is being transmitted, possibly unbeknownst to the user. The user can subsequently disable the transmissions of data that he did not approve. While this provides the user with a certain degree of control over what of his data – potentially personal data – is being transmitted, it also raises the question on whether the user should not be asked to opt-in to such information transmission instead of having to opt-out from it.

3.2 Smart Office Scenario

While the actual applications of the Smart Office and the Smart Home are rather similar, they stem from different goals and could therefore have different technical and legal implications. As a result, the Smart Office scenario was developed separately from the Smart Home scenario.

First, the project meeting application describes the need for security and access management. Employees and visitors must be granted appropriate credentials, links to infrastructure, vouchers, access to certain facilities and this sometimes for specific periods of time. The access management and technologies used – such as Bluetooth and NFC – raise similar questions as under the Smart Home scenario. Additional questions are raised with regards to the invitations and credentials. One will need to establish their authenticity and integrity to assess their value and origins. This relates to the implication of the legal value of electronic information, as discussed earlier. Also connections to the meeting infrastructure – such as projectors and printers – and taking secure notes relate to access management. However, as all this access management could lead to a great number of recordings – for instance when somebody enters through a door – one needs to ensure that the legal provisions regarding privacy and data protection on the work floor are respected.

With regards to meeting partners, the data subject should be given the competence to – up to a certain level – decide which of his personal data he wants to share. Such correspond to the legal requirements with relation to data protection as discussed under D7.1 Legal Requirements for Trust in the IoT. Also here, technologies such as Bluetooth and NFC are used to establish device communication.

While the possibility for remote meeting participation in part also relies on access rights, there is an important deviation. The scenario provides for digital resources sharing, in which the original request for data sharing included a back-up service. Important is that the user can change this request at will, leaving out the option of backing-up personal data on a remote server, before accepting. Such would

provide the user with an important competence not to be confronted with nonnegotiable requests that require sharing of data that the user does not want to share.

A second scenario, the Smart Break Room, allows for employers to securely purchase snacks and beverages. Using NFC, the uTRUSTit device could communicate an employer's choice of beverage to the vending machine and subsequently pay for the purchase. Again, the technologies used and the use of electronic payment will have to be further analyzed from a legal point of view.

3.3 Summary

Given the many similarities between the goals and needs of the personas developed within this project and the scenarios subsequently developed to visualize a solution to these goals and needs, the legal implications that were extracted from the scenarios correspond fully to the legal implications extracted from the analysis of the personal performed earlier under chapter 2 of this deliverable.

In short, the legal implications stemming from the scenarios can be divided into a number of categories. First, the implications regarding data protection relate to how personal data is processed and to how privacy is respected, both at work and at home. These implications were found in both the Smart Home and the Smart Office scenarios.

Second, a number of elements – mainly the use of the Trusted Smart Home health monitor – raise questions with regards to consent. How can informed consent be effectively given here and are certain persons still legally capable of providing their consent?

Third, the health monitor raises further concerns with regards to the adaptability of its features to the user's wishes and with regards to its processing of health data.

Fourth, both the Home Entertainment Management application and the Smart Break Room make use of online payments. Here, one will have to ensure that such payments are trustworthy executed. Existing provisions relating to, for instance, e-commerce and the legal value of electronic information could aid in securing the trustworthiness of online transactions.

Fifth, security and access management is one of the most important features of both the Smart Home and the Smart Office scenario. Also here, one will need to assess how such access management can be performed fully legally compliant.

Sixth, one will have to set the requirements to the technology that will be used in realizing the applications envisioned here. These technologies include RFID, GPS, NFC, Bluetooth and Wi-Fi.

Last, the borders between providing access to a home media center and illegitimate file sharing have to be guarded in order to provide the uTRUSTit applications from being used as a potential copyright infringement.

4. Development of Legal Requirements

In the analysis of the personas developed within this research project and of the visualization of their needs and goals in the home and office scenarios, a number of legal implications were derived from this information. These legal implications will be further analyzed in order to be developed into legal requirements to which the prototype of the Smart Home and Smart Office scenario will have to adhere, in order to ensure their legal compliance.

The basic legal requirements formulated in Deliverable 7.1 – Legal Requirements for Trust in the IoT – will be further developed here with specific attention to the precise legal implications set by the personas and the scenarios analyzed. For the purposes of maintaining an easy overview for non-legal specialists, the general and more specific legal requirements developed here will be consolidated under chapter 5 – Consolidation of Legal Requirements – of the present deliverable.

4.1 General data protection requirements

Analysis of the personas and the scenarios demonstrated a number of legal implications with regards to data protection. While the general European legal framework regarding the processing of personal data was already covered under the previous legal deliverable – D7.1 Legal Requirements for Trust in the IoT – the basic legal requirements developed there will have to be applied to the specific situations in terms of needs and goals of the personas and the visualization of potential solutions in the scenarios. For instance, it will have to be analyzed what the influence is of the use of assistive technologies in processing personal data as part of one's job.

An important thing to note here is that privacy related requirements should not only be aimed at professional processing of personal data. For instance, if one wants to keep track of one's family's appointments or Internet behavior, one could also be processing personal data. While such would occur in a household setting – thus possibly benefiting from an exception to the general obligations under European data protection legislation – one should still bear in mind general privacy provisions.

4.1.1 Data protection and privacy at home

A number of elements expressed in the needs and goals of several personas and in the Smart Home scenario indicated legal implications with regards to the protection of the privacy of people at home, as well as possible processing of the personal data of these people in a private setting. For instance, the Trusted Smart Home provides for access management, which can include the logging of the access habits of the people living in that home. Also the request for a tool to manage all appointments of different family members may be considered to be intrusive to the personal sphere of certain of these family members. This is even more the case for the expressed desire to monitor the online activities of one's children. One will therefore have to analyze how such practices would have to comply with existing legal provisions regarding privacy and data protection at home.

As already analyzed under D7.1 - Legal Requirements for Trust in the IoT, article 3 (2) of the Data Protection Directive[4] provides for an exception that states that the directive does not apply to the processing of personal data

> *by a natural person in the context of a purely personal or household activity.*

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , *OJ* L 281 of 23 November 1995, 31-50 (hereinafter: Data Protection Directive).

This exception is commonly referred to as the 'household exception' and allows for natural persons to perform what can be regarded as a processing of personal data, as long as such processing serves strictly personal intent.

For the application of the household exception, it is imperative that the person processing certain types of personal data acts in a personal capacity and that his processing serves only purposes of his personal or household sphere. One of the defining elements to establish personal capacity and personal sphere purposes was found in case law, where the ECJ ruled that the publicity of the information is a defining aspect of the household exception.[5] If, for instance, the personal agenda of all family members is published on the Internet with no access restrictions, this data will be considered as having become publicly available. As a result, the household exception can no longer apply to the processing of this data.

One can summarize this as follows:

> **Req. B1[6]: Processing of personal data of family members of the same household is required to be executed in a personal capacity and strictly for purposes in the personal or household sphere, with restricted publicity of this data. Failure to observe personal capacity, personal or household purposes or to keep data publicity limited will result in the non-applicability of the household exception. As a result, the processing of this personal data will have to comply fully with all personal data processing requirements.**

However, the previous only covers situations in which actual personal data is processed. Certain elements – such as the monitoring of a child's online activities – do not necessarily require the processing of personal data, thus not necessitating the applicability of the household exception. However, they can pose a rather substantial intrusion of the personal sphere of the child. Also with regards to the logging of who accesses the home at what hour could pose an infringement to a person's privacy, even if the personal data potentially processed in this act would be covered by the household exception.

Such monitoring activities may even pose an infringement to criminal law. In Belgium, for instance, private telecommunication is protected by article 314bis of the Criminal Code. This article is aimed at everybody who willingly takes notice of the contents of a private telecommunication to which he is no party, during its transmission and without prior permission of all participants to the communication. Given the broad scope of this article, private telecommunication can also include communications through the Internet [DUMORTIER 2010]. However, note that for the scope of this article, it is important that the notice of the contents of the private telecommunication needs to be taken during its transmission. Looking into a child's saved chat logs, for instance, will not be covered by the scope of this article.

However, by taking notice of the contents of the private telecommunication, one obviously also takes notice of the existence of that private telecommunication, which is another criminal act according to article 124 of the Electronic Communications Act[7]. This article concerns the situation in which one deliberately takes notice of the existence of online communication to which this person is not a party and without having received prior permission from all participants to that communication. Such could include the monitoring of a child's Internet activities by its parents without prior consent of the child

[5] ECJ C-101/2001 Bodil Lindqvist, 2003, §46-47; ECJ C‑73/07 Tietosuojavaltuutettu *v* Satakunnan Markkinapörssi Oy & Satamedia Oy, 2008, §44.

[6] Note that the numbering of the requirements used throughout this document corresponds to the consolidated requirements found under chapter 5-Consolidation of Legal Requirements.

[7] Act of 13 June 2005 regarding electronic communications, *Belgian State Gazette* 20 June 2005.

and its communication partners. As parents are in theory the legal guardians of their children until they reach the age of majority, such consent would in principle not be required. This is, however, a legal grey area in which one would have to assess the level of maturity and accountability of the minor. If, for instance, parents have entrusted their minor child with unrestricted Internet access, one could argue that the parents have conferred a certain level of responsibility unto it, which would in turn require the parents to receive prior permission before checking in on its online activities.

Also general privacy law can oppose such monitoring of online activities, personal agendas and home access habits. For one, article 8 (1) of the European Convention on Human Rights[8] specifically states that

> *everyone has the right to respect for his private and family life, his home and his correspondence*,

which also applies to children[9]. Specifically for minors, there is the United Nations Convention on the Rights of the Child[10], which states in its article 16 that

> *no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence.*

Given the wide acceptance of this convention by UN Member States and their subsequent ratification of that instrument, one can expect to find similar provisions in national legislation worldwide.

While it should be noted that human rights conventions are generally conceived as including *vertical* obligations – i.e. obligations of a State towards it citizens – there is already enough consensus on the possibility of *horizontal* obligations – thus between private citizens [BESELINK 2003; VANWIJNGAERDEN 2008]. Especially the European Convention on Human Rights has to be regarded as being an important instrument, given its importance in drafting the Charter of Fundamental Rights of the European Union.[11]

As a result, the general right to privacy – even when no processing of personal data is involved – will protect the privacy of children and other family members. While children that have reached the national age of maturity are protected as any other adult, it is clear that also minors have their personal right to privacy. Consequently, every unwanted intrusion to the private life of family members of the same household – including with regards to their communications – will be a violation of their right to privacy. Therefore, the home access monitoring, agenda sharing and Internet activity monitoring can only be executed upon being granted prior consent of each individual concerned.

> **Req. B2: Also when no personal data is processed or when the household exception applies, any intrusion to the personal sphere of family members – including minor children – will be considered as a violation of their privacy. Prior consent must therefore be granted.**

4.1.2 Data protection and privacy at the office

As the Smart Office scenario presented IoT solutions that were rather similar to what was analyzed under the Smart Home scenario – access management and logging, collaborative technologies and activity monitoring – similar legal implications can be formulated as well. The main difference in an office environment is that the household exception regarding the processing of personal data for personal or household purposes cannot apply in such setting. As a result, all processing of personal data executed in an office environment will need to be fully compliant to the general rules on data protection.

[8] Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950.
[9] Specifically addressed by the European Commission: Commission Green Paper of 16 October 1996 on the protection of minors and human dignity in audiovisual and information services, *COM(1996) 483*, 12.
[10] United Nations Convention on the Rights of the Child, 20 November 1989, A/RES/44/25.
[11] Charter of Fundamental Rights of the European Union, *OJ* C 83 of 30 March 2010, 389 *et seq*.

The general European framework on data protection was analyzed under D7.1 – Legal Requirements for Trust in the IoT. The general requirements developed there can be applied to this particular situation. The following list of requirements can therefore be re-used and will – later on in chapter 5 (Consolidation of Legal Requirements) of this deliverable – be expanded and further coordinated using the more specific requirements that will be developed here:

Req. A1: It is required that IoT actors identified as data controllers should be aware of the precise definitions of national data protection legislation applicable to the processing under their control.

Req.A2: The data subject's free, informed and unambiguous consent is required for legitimate processing of personal data.

Req. A3: Legality or transparency is required for fair and lawful processing of personal data.

Req. A3: The purposes of the processing of personal data are required to be clearly indicated in advance.

Req. A5: The processing of personal data is required to only include relevant and non-excessive data, in relation to the specified purposes.

Req. A7: The data controller is required to ensure sufficient information of the data subject.

Req. A8: The data controller is furthermore required to ensure that the data subject can fully enjoy his right of access, his right to correction and his right to object.

Req. A9: Special notice is required to the special categories of personal data.

Req. A10: The data controller is required to ensure confidentiality and security of the processing of personal data under his control.

Req. A11: Due notification to the competent national Data Protection Authority (or Authorities), in compliance with national legislation, is required.

Req. A12: Data transfers to third States are required to comply with applicable legislation.

Similar to the analysis performed for the Smart Home scenario, one will also have to keep in mind general privacy provisions. Even though the Smart Office cannot be regarded as a personal or household setting – thus the non-applicability of the household exception with regards to personal data processing – it is generally accepted that employees have a certain right to privacy on their work floor. Also article 8 of the European Convention on Human Rights is said to apply on the work floor, as found in case law by the European Court of Human Rights (ECHR).[12]

As the protection of private telecommunication[13] – as found in the Belgian Criminal Code and the Belgian Act on Electronic Communications, as discussed under chapter 4.1.1 (Data protection and privacy at home) of the present deliverable – makes no direct exception to telecommunications on the work floor, one should consider this principle to apply to telecommunications on the work floor as well [DUMORTIER 2010]. However, as an agreement to employment implies a certain authority of the employer over its employees, he will be able to exercise some control over the telecommunications in

[12] ECHR 62617/00 Copland *v* the United Kingdom, 2007, §§ 41-42.
[13] Also addressed as communication secrecy [WORKING PARTY 55].

his business. As a result, the Belgian Labour Council adopted a collective labour agreement regulating the protection of the privacy of employees with regards to electronic communications.[14]

The collective labour agreement holds that an employer can decide on which means for telecommunications can be used on his work floor, without hindering the employees' right to private telecommunications. While the employer may set rules on the use and on the control of these means for telecommunications, he will have to ensure that such rules are sufficiently transparent and that they comply with the general principles regarding data protection, as monitoring such telecommunications may include the processing of personal data. Most importantly, the collective labour agreement holds that the monitoring of telecommunications can only occur for four specific purposes: (1) the prevention of unlawful or slanderous facts, that could damage the moral or dignity of another person; (2) the protection of economical and financial interests of the company; (3) the safety and good technical functioning of the network systems of the company, including the monitoring of its costs and the physical protection of installations and (4) the *bona fide* compliance with the rules and provisions regarding the use of online technologies as applicable in that company. In the first three cases, the employer can monitor the data of one specific employee. In the case of general monitoring (4), the employer must first warn the employee before he can monitor that specific employee [DUMORTIER 2010].[15]

While this collective labour agreement obviously only applies to Belgium, it should be noted that also the Article 29 Working Party has adopted a number of texts assessing the right to privacy on the work floor. One text in particular relates to the surveillance of electronic communications [WORKING PARTY 55]. In this document, the Working Party confirms that employees can have reasonable expectations of privacy on their work floor, which needs to be balanced with the employer's interests regarding the running of his business and regarding liabilities. To that result, article 8 of the European Convention on Human Rights and Directive 95/46/EC are fully applicable to an office environment.

With regards to e-mail monitoring, it is stated that such can only be done if such is absolutely necessary, which will only occur in rare cases [WORKING PARTY 55]. The principles of Directive 95/46/EC regarding finality, transparency, legitimacy, proportionality and data subject's rights are fully applicable. While monitoring of an employee's e-mail account cannot be fully ruled out, the Working Party advises to maintain a policy in which employees can use private webmail accounts for their private communications, next to their professional e-mail account.

For Internet monitoring, the Working Party advises prevention of Internet access misuse by technical means. Such would limit the need to actual monitoring of an employee's Internet activities. For instance, by monitoring which websites are most visited by an office the employer can get an idea of potential Internet access abuse without having to monitor all employees' traffic. An Internet Policy could lay down a number of ground rules and should be made fully transparent to the employees.

While the general data protection provisions normally require the data subject's prior and informed consent, the Working Party finds that such consent is of no value in an unequal relationship such as between an employer and his employees. Consent should therefore be reserved for cases in which the employee truly has the free choice to give his consent, as well as to withdraw that consent when he changes his mind. Free consent would also include the possibility to negotiate or to alter the situation to which one's consent is needed. In the scenarios, for instance, this was expressed by the possibility to change a request for digital resources sharing [UTRUSTIT 2011c], for which the original request for data sharing included a back-up service. In the scenario, the request was changed at the will of the user, leaving out the option of backing-up personal data on a remote server, before accepting. Such provides the user with the competence to negotiate requests in order to provide his truly free consent.

[14] Collective Labour Agreement nr. 81 of 26 April 2002 regarding the protection of the privacy of employees with regards to the monitoring of electronic communications data, *www.nar-cnt.be*.

[15] The idea of prior notice of monitoring activities can also be found in article 6.14 of the International Labour Office's Code of Practice on the Protection of workers' personal data [ILO 1997].

The Working Party has provided a list with a number of requirements for the processing of personal data of employees, which corresponds well with the requirements already listed here [WORKING PARTY 48]. In order to provide a more complete overview, the requirements formulated by the Working Party will be listed here as well:

> **Req. A5: Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.**
>
> **Req. C1: As a very minimum, workers need to know which data the employer is collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future. Transparency is also assured by granting the data subject the right to access to his/her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.**
>
> **Req. C2: The processing of workers' personal data must be legitimate. Article 7 of the Directive lists the criteria making the processing legitimate.**
>
> **Req. C3: The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker.**
>
> **Req. C4: Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified.**
>
> **Req. C5: The employer must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access.**
>
> **Req. C6: Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.**

In summary, one will find that the processing of data regarding employees will inevitably include personal data, in which case such processing will need to comply with the general provisions regarding data protection. Personal data will also be processed when monitoring employees' activities. Furthermore, the general right to privacy is regarded as also applying on the work floor, thus requiring a balance between the exercise of this right by the employee and the legitimate interests of the employer in efficiently running his business. Also the right to communication secrecy will need to be respected.

There is, however, another aspect relating to the processing of personal data on the work floor. While the previous analysis only focuses on an employer's processing of the personal data of his employees, the business activities of the employer may also require the processing of personal data, for instance of customers. As a result, such processing will also have to comply with the principles set forth by Directive 95/46/EC.

First, it is important to determine the capacity in which an employee performs personal data processing for his employer. In general, employees will perform such processing as part of the execution of their obligations under their agreement of employment with their employers. Subsequently, it will be that employer that acts as the actual data controller of such processing. As part of their agreement of employment, most employees will be directly subjected to their employer and will thus not be an external party contracted for this processing. As a result, regular employees will not be considered as being the processor of such personal data processing. While not being the actual controller or processor of the personal data processing, employees must comply with the means and purposes on the processing of personal data determined by their employer.

With regards to the assistive technologies mentioned in the scenarios, it will be important to know whether and how they comply with those means set by the data processor. A screen reader could, for instance, log the data it is being fed for conversion to speech. If such data logs would exist, they could also include personal data. As a result, it would be important to assess how and for what period of time such logs are stored, for what purpose, what data they contain precisely and by whom they can be accessed.

Here, one will have to assess how the assistive technologies used by Anna fit into the requirements set to the processing of personal data. For instance, does the screen reader log the data it reads to Anna? If so, it will be important to know how such logs are stored and who can access them.

This can be summarized in the following requirements:

Req. C7: The precise capacity in which one party performs personal data processing on behalf of another party must be clearly established. Employees must be clearly identified as such in order to distinguish them from their employer/data controller and the external processor.

Req. C8: In order to determine their compliance with the means and purposes of a personal data processing, assistive technologies must clearly indicate whether, how and for what period of time logs containing personal data are stored, for what purpose, what data they contain precisely and by whom they can be accessed.

4.2 Informed consent requirements

The analysis of the personas and the scenarios demonstrated a number of legal implications with regards to consent. While consent is generally understood as being an integral part of the general European legal framework regarding the processing of personal data – and was therefore already analyzed under D7.1 Legal Requirements for Trust in the IoT – the specific situations in terms of needs and goals of the personas and the visualization of potential solutions in the scenarios demonstrate certain legal implications that require the general legal requirements relating to consent previously developed to be analyzed deeper and to be developed further.

It is in particular the Trusted Smart Home health monitoring system that gives rise to these legal implications with regards to consent. While the health monitoring system itself will be analyzed as well – under chapter 4.3 – Health monitor requirements – the specific issue of consent should be addressed separately as consent is an important element in all types of personal data processing and potential privacy infringements.

In the analysis of the needs and goals of the personas and of the possible solutions developed in the scenarios, two specific issues relating to consent were identified: How can informed consent be effectively given here and are certain persons still legally capable of providing their consent? While this chapter will analyze the general legal background regarding consent and legal capacity, one should also

refer to national law for the specific requirements regarding legal capacity and possible delegations thereof as such is not regulated at a European level.

4.2.1 Effectiveness of consent

From the analysis of the personal attitudes of the personas towards new technologies, it became clear that privacy policies and consent forms are not often fully read, let alone fully understood. This attitude may stem from a general sense of mistrust in new technologies, or unfamiliarity therewith, which eventually leads to the perception that the technical aspects of the technology and the legal aspects of the privacy policies and consent forms are too difficult to grasp. Alternatively, one can also distinguish people with a feeling of overconfidence in technology, which will not read privacy policies and consent forms because they trust that technology will not harm them. While these personal attitudes may be rather divergent, they do lead to the same consequence: by not reading or understanding privacy policies and consent forms, both types of persons are exposed to the risk of providing consent without knowing to which they consented.

The problem created by these attitudes towards consent forms and privacy policies demonstrates two underlying issues.

First, privacy policies and consent forms are often regarded as being too technical or legal, thus becoming almost unintelligible to people without a strong technical and/or legal background. Consent forms and privacy policies must therefore be drafted keeping in mind their target audience, which mostly consists of people that have no particular experience with technology and that are not legally trained. Also, one should pay attention to the presentation of the consent form or privacy policy. A long and detailed text is less likely to be read than a comprehensive and structured overview. However, as the level of detail in the text is often the result of legal obligations to include all information needed for the data subject to provide his fully informed consent, one should try to strike a balance between these legal obligations and the need of many people to be presented a comprehensible privacy policy or consent form.

Second, one should look into the effectiveness of privacy policies and consent forms. This becomes especially apparent in the context of the Internet, where a simple 'click-to-accept'-button will lead many users to clicking that button without having read the text, thus consenting to the processing of their personal data, unaware of the specifics of such processing. One should therefore try to device a way of ensuring that privacy policies and consent forms are fully read and understood before acceptance, while on the other hand maintaining a level of user-friendliness.

The Data Protection Directive – Directive 95/46/EC – lists a number of grounds that can legitimate the processing of one's personal data. However, most of these grounds will only apply in a limited number of relatively rare cases, thus making the first legitimization ground, informed consent, the most valuable ground for a legitimate processing of personal data. While this idea of consent was originally viewed as an expression of the right to informational self-determination of the data subject and of user empowerment, the rise of electronic communications and its reliance on consent has lead to a certain undervaluation of this concept [KOSTA 2011]. While the situation described here leads to the questions as to how the data subject should be adequately and understandably informed and how the data subject should express his consent, one could also question whether consent is still an adequate tool for user empowerment and informational self-determination. While certain provisions[16] already indicate that consent may one day serve a less important role, such change is not likely to be implemented in the European legal framework on data protection soon.

For the time being one will still have to obtain the data subject's informed consent, thus warranting the development of a set of criteria regarding how to properly inform the data subject in order to receive his consent and regarding how to ensure that the data subject has actually read and

[16] For instance, the Swedish exemption of unstructured processing of personal data results in Internet users not being required to obtain consent from every person they mention in their online activities [KOSTA 2011].

understood all information given to him before granting his consent. As defined by the Data Protection Directive, informed consent needs to be given freely and specific. The matter of freely given consent will be explored further in the following chapter of this deliverable, chapter 4.2.2 – Capacity to consent.

Requirements relating to the provision of adequate information to the data subject were already developed under the previous deliverable D7.1 – Legal Requirements for Trust in the IoT. There, it was found that a layered approach – with a short, a condensed and a full notice – would be the most adequate way to inform the data subject and to receive his consent. Also standardized forms were encouraged to ensure that all privacy policies and consent forms are similarly accessible.[17]

The requirements developed before can be summarized as follows:

> **Req. D1: Carefully drafted privacy policies and consent forms – for instance in a multi-layered format – are required to ensure compliance to the requirement of consent and the right to information. Note that such privacy policies and consent forms need to be compliant with national data protection legislation. For instance, certain jurisdictions require written consent, while others allow for implicit consent in many cases.**

Such layered consent form should already make the form more readable and accessible to a larger non-technical and not legally trained audience. However, one will still need to ensure that the people that normally ignore consent forms and privacy policies are now persuaded to actually read such information before granting their consent. Here, one could think of technological measures that could be implemented to, for instance, require the user to scroll through the privacy policy before being able to grant his consent. Imperative here is that user-friendliness is observed. Most users are not likely to be willing to spend a lot of time going through the procedure of granting consent before being able to use a service, such as a social network. A balance needs to be struck between the legitimate interests of the data controller – for which he needs the data subject's consent – and the privacy of the data subject [KOSTA 2011].

> **Req. D2: User-friendliness must be the focal point in obtaining the data subject's consent. While unintelligible texts may lead to the data subject not reading a privacy policy or consent form, elaborate procedures to grant consent may result in the data subject refraining from using such service, thus damaging the business of the data controller. A balance between the interests of both parties must therefore be struck.**

4.2.2 Capacity to consent

As already indicated, a second component of the consent issue concerns the capacity to give one's consent. Also, as the Data Protection Directive requires consent to be given freely, one should look into whether consent can truly be given freely. For instance, as found in the scenarios, elderly persons with health concerns could be subjected to a health monitoring system in order to maintain a certain level of independence. The question is then whether such trade-off still be considered as freely given consent. Also, as the specific case developed in the scenarios here involves a person with onsets of dementia, one should ask whether such person can still be considered as capable of providing consent.

[17] Communication of 4 November 2010 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "A comprehensive approach on personal data protection in the European Union", *COM(2010) 609*, 6.

While the Data Protection Directive does not directly refer to the capacity of the data subject to grant his consent, there is a provision that allows for personal data processing to protect the vital interests of the data subject when he is physically or legally incapable of granting his consent.[18] This provision relates to the processing of so-called sensitive data, which in principle is prohibited and can only occur in a select number of strict cases. Such may give an indication of the need to have the legal and physical capability to provide informed consent.

This problem also becomes apparent when the data subject is a minor. While minors in principle do not have legal capacity, they may already have certain legal competences under different national legislations. The national differences regarding age and scope of legal competence of minors makes it difficult to establish a common point of view regarding the capability of minors to grant their consent to the processing of their personal data. One could therefore recommend seeking consent of both the minor data subject and its parents or legal guardians [KOSTA 2011]. Such would also assist in securing validity of the consent when this validity is being judged in court.

As it is clear that the data subject's statutory or legal representative can provide consent for the data subject, this would indicate a similar situation to that of minors: while the legal capacity of elderly, especially when facing a mental illness, depends on divergent national legislations and would have to be judged on a case-by-case basis, one could best seek the consent of both the data subject and his legal representatives, where available.

> **Req. D3: When dealing with minors, elderly and/or persons with a mental illness, the data controller is advised to seek consent from both the data subject and its statutory or legal guardians. The general legal capacity of the data subject determines its capacity to consent.**

As a person's mental state can also change over time, one may argue in favor of consent with limited duration. In such case, consent should be regularly renewed. This is specifically important for cases of continuously ongoing processing of personal data.

> **Req. D5: Consent should be limited in time and should be renewed for continuously ongoing processing of personal data. Consent should also be revocable.**

Second, the Data Protection Directive requires consent to be given freely, without any third party pressure. Such third party pressure or influence, however, can be found in many places. For instance, one can think of the unequal relationship between an employee and its employer. As one party, the employer, clearly has the beneficial position in the relationship, one may ask whether an employee is truly free to consent on the processing of his personal data.

As a result, one may even question the use of requiring consent in such unequal relationships. With regards to the processing of personal data of employees, the Article 29 Working Party holds that

> *reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment* [WORKING PARTY 48].

In unequal relationships, it would therefore be advised to seek a different ground for personal data processing, as freely given informed consent – as required by the Data Protection Directive – cannot be provided.

One should, however, make a distinction between the types of external pressure exercised on the data subject. One may distinguish positive pressure and negative pressure [KOSTA 2011]. If the person, for instance, knows he can expect a certain benefit from granting his consent, he was externally influenced. However, if he was properly informed and still had real freedom in deciding on whether to consent or not, this positive pressure cannot be seen as invalidating his freely given consent. However,

[18] Art. 8 (2)(c) Data Protection Directive.

when duress is employed, it is clear that the data subject's freedom of choice was limited, thus invalidating his consent as it could not be truly freely given. External pressure on the data subject's consent should therefore be classified as being either coercive or persuasive, with the former being negative pressure and the later being positive pressure.

> **Req. D4: Informed consent must be given freely. In order to determine whether the data subject's consent was given freely, one needs to analyze the external pressure exercised on his decision. Positive persuasion cannot invalidate his freely given consent, while negative coercion will invalidate his consent as it could not have been given freely.**

4.3 Health monitor requirements

One of the main features developed under the Smart Home scenario is the Trusted Smart Home health monitoring system. While such system certainly promises practical benefits to the person that requires health monitoring, his relatives and healthcare workers, there are also a number of legal questions to be formulated with regards to the precise workings of such system.

First, as it is clear that such system may include the processing of personal data and as it poses an intrusion to the monitored person's private life, it would be advised to obtain that person's consent. As already analyzed under the previous chapter, obtaining the consent of a person that requires medical surveillance may pose problems with regards to his capacity to consent and whether such consent was freely given or was the result of certain coercion. The specific legal requirements resulting from this analysis were formulated under the previous chapter.

Second, the scenario shows a large number of features that could be included under the umbrella of the Trusted Smart Home health monitoring system, such as home access control and management, medicine management and location tracking. As each of these features poses an individual intrusion to the private life of the person under surveillance, one should ask whether all of these features are necessary and whether they really need to be active continuously. This raises questions with regards to the adaptability of the features of this system to the user's wishes and with regards to its processing of personal data.

Third, as the scenario demonstrates that this system is capable of collecting and processing substantial amounts of data, amongst which also personal data, and as this system is specifically aimed for use in a medical context, one may assume that health data concerning the person under surveillance will be processed. As this type of personal data has been considered as a special category of personal data under the European legal framework on data protection, one will have to assess whether specific requirements and procedures go accompanied with it.

4.3.1 Adaptability of the health monitoring system

A first question to be answered here is whether it can be found acceptable that the health monitoring system continuously processes large amounts of data, amongst which personal data and whether the system should be adaptable to the specific needs and desires of the data subject. Can the purpose definition of health monitoring justify that a person is monitored at all times for an unspecified period of time? Is it acceptable that a person's consent to being monitored for health purposes exposes him to a number of additional features, some of which may be considered as intrusive?

To answer this question, one will have to refer to the principles relating to data quality as found under article 6 of the Data Protection Directive. This article states that personal data must be processed fairly and lawfully, for specified, explicit and legitimate purposes, that only accurate and up-to-date data may be processed in an adequate, relevant and non-excessive manner and with storage no longer than necessary for the purposes of the processing. These provisions may aid in determining the scope of the health monitoring system with regards to data protection and the possibility of user adaptation.

First, one must examine the proportionality principle, which underlies much of the principles relating to data quality of the Data Protection Directive. This principle holds that one needs to balance the legitimate interests of the data controller and those of the data subject by ensuring that an excessive intrusion to the data subject's privacy is avoided. Therefore, it must be assessed whether the means used in the processing – *in casu* the house access management, the medicine management and the location tracking – are really suitable and necessary for the purposes of the processing – *in casu* the health monitoring – and whether there are no other options available which would yield the same result but that would be less privacy intrusive.

It should be noted that the proportionality principle covers broad grounds. As a result, it is not limited to assessing whether the means are suited and needed for the purposes, but also encompasses the idea of data minimization. This means that only the data that is strictly necessary for the purposes may be processed. An important distinction made here is whether there is a *need to know* for the data collected or whether that specific data is just *nice to know* [VAN ALSENOY 2007].

The proportionality principle also includes storage duration, as processed personal data can only be stored for as long as necessary for the purposes of the processing. The scenario developed for the Trusted Smart Home health monitoring system indicates that the system only processes data for a specific action, for instance activating the access management system, emitting a warning signal or displaying a reminder. Once such action is completed, the purpose for which the data was collected has been achieved and therefore the data can no longer be stored.

Also with regards to use, it should be reminded that the collected data can not be used for other purposes than to which the data subject consented upon collection and of the purposes notified to the competent data protection authority.

As a result, one may have to assess the proportionality of the different features of the Trusted Smart Home health monitoring system and their potentially continuous monitoring on a case-by-case basis. A number of features – such as the tracking system and the fall detector – are in principle only activated in case of emergency. As a result, they should only process data when activated. As no data is processed when these features are inactive and as they are only activated when necessary, the processing performed by these features could be considered as being proportional as it does not demonstrate excessive personal data processing. This can be summarized in the following requirement:

> **Req. E1: In using technologies that could potentially lead to a continuous collecting and processing of personal data, one must assess the proportionality of such collecting and processing. Mostly, the purpose for which the technology is used and for which the data is processed does not necessarily require continuous data processing. Therefore, one must select the least intrusive yet suitable means that lead to minimal data collection and storage.**

With regards to the adaptability of the features of the Trusted Smart Home health monitoring system to the data subject's preferences, one could refer back to the previous chapter on the data subject's consent. As such consent needs to be given freely, without external force applied to it, the processing to which he consents – and thus including the means and purposes of that processing – needs to be negotiable. If the data subject was coerced into consenting by his unbeneficial position, his consent will be void. The idea that the processing and its means and purposes need to be negotiable, demonstrates that the data subject can object to certain parts of the processing. For instance, within a health monitoring system, the data subject could consent to a fall detector that is only activated to collect data upon detecting a fall, while rejecting consent for a tracking device that is set to continuously monitor his movements. Also, as consent is revocable, the data subject may at any time decide to halt certain parts of the processing.

As a result, one may find that the data subject should be offered the option to disable the options that are, in his personal conviction, too intrusive to his privacy. Such disconnection could be temporary or on a more permanent basis. This corresponds with an idea coined by the European

Commission to establish a right to silence of the chips, which would give the data subject the right to disconnect from his networked environment at any time.[19] In fact, the Commission explicitly referenced a household health monitoring system and added that it is a

> *…prerequisite for trust and acceptance of these systems* […] *that appropriate data protection measures are put in place against possible misuse and other personal data related risks.*[20]

This analysis can be summarized into the following requirement:

> **Req. E2: As consent requires certain negotiability and as consent can be revoked, the health monitoring system must allow for certain adaptability of the system to the specific needs and wishes of the person under medical surveillance. This person must be offered the option to – temporary or permanently – disable the features that he deems to intrusive.**

4.3.2 Processing of health data

The second problem to be discussed here, concerns the data that will be processed in the Trusted Smart Home health monitoring system. As the concept of personal data needs to be interpreted rather broadly as in every data that could directly or indirectly lead to the identification of a natural person, one can expect the Trusted Smart Home health monitoring system to also process personal data. More importantly, this particular system concerns data relating to a person's medical condition, which is part of what the Data Protection Directive addresses as a special category of personal data, also known as sensitive data.

As discussed under D7.1 – Legal Requirements for Trust in the IoT, the concept of sensitive data can be interpreted very broadly. As the Data Protection Directive itself does not give a clear definition of the precise scope of this concept, one will have to look at interpretations and implementations by Member States. Here, it was found that a broad interpretation of the concept of sensitive data can certainly be defended, yet that this concept should not be stretched to its broadest sense, as such could lead to undesirable results [UTRUSTIT 2011b]. As a result of the broad definition of the concept of sensitive data, one can consider that certain of the data collected by the health monitoring system can be considered as being medical data, thus being sensitive data. Also the fact that all of this data is collected with the main purpose of monitoring a person's health is an indication of the medical nature of this data.

First, however, one needs to assess the applicability of the Data Protection Directive to this specific situation. The scenario describes the monitoring of a person within his own household, with his own consent and with the health monitoring system mostly being under the control of that persona's son. Such could lead one to think that the household exception may apply here, as the processing is mainly performed within a household sphere. The involvement of external parties – the healthcare workers that operate under their employer, a private healthcare organization – that also play a role in the monitoring process, however, rules out the applicability of the household exception. The processing of personal data performed under the health monitoring system will therefore be fully covered by the scope of the Data Protection Directive and will have to comply with its specifications.

Being sensitive data in the sense of article 8 of the Data Protection Directive, health data will need to be processed in accordance with one of the exhaustively listed justification grounds provided under article 8 (2). One possible justification ground applying to the health monitoring system is that of the data subject's explicit consent, which has been interpreted as written consent by certain Member

[19] Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "Internet of Things — An action plan for Europe", *COM(2009) 278*, 5-6.
[20] *Ibid.*, 6.

States. One could also look at the processing necessary to protect the vital interests of the data subject where he is physically or legally incapable of giving his own consent. This, however, would require the person under medical surveillance to be declared legally incapable and being put under the custody of a legal guardian. Another exemption for the processing of health data requires that the processing is performed by a health professional and can therefore not apply to this case.[21] As a result, the most viable justification ground for the processing of the health data of the person under medical surveillance will depend on his legal capacity to consent. As long as the data subject can legally give his own informed consent, such consent will serve as the only justification ground for the processing of his health data in the context of a health monitoring system. When he has been declared incapable of giving his consent, such processing can only be performed if it can be proved to be necessary for the protection of the data subject's vital interests. This can be summarized in the following requirement:

> **Req. E3: When health data is processed as part of the health monitoring system, the data controller is required to obtain the explicit – or written, where applicable – consent of the legally capable data subject as justification ground for the processing of this special category of personal data. In case of legal incapacity of the data subject, the processing of his health data can be performed if necessity for the protection of his vital interests can be demonstrated.**

For the requirements relating to the actual processing of health data, one can refer to the general requirements relating to the processing of personal data. The processing of special categories of personal data only deviates from these general requirements in terms of justification grounds.

4.4 Electronic payments requirements

In today's society, more and more transactions no longer require the physical exchange of goods against cash payment, but rather rely on the electronic exchange of goods and services against electronic payments. Notable examples are the many application stores that provide software applications for different smartphone platforms. Even when a physical good is still transferred to the buyer, such as is the case for a vending machine, payment for these goods will more and more be achieved through electronic means. The scenarios developed within the uTRUSTit project reference a few cases in which electronic payments are made. First, there is the vending machine found in the Smart Break Room, where one's uTRUSTit device can be used for both placing an order and for payment. In both cases, the device is waved over the appropriate area of the vending machine, thus completing the purchase without any physical contact. A similar case can be found in the Trusted Smart Home Entertainment Management application, where media data can be purchased and delivered electronically, thus requiring no physical contact between buyer and seller. Second, this scenario can be expanded to a broader context of vending machines, parking meters and Automated Teller Machines (ATMs), which are found in a public and thus incontrollable environment. Many public transport companies, for instance, are currently transgressing from distributing physical tickets to virtual tickets, purchased through electronic transactions. As such transactions are performed in a public and incontrollable environment, the need to know the trustworthiness of such transactions is heightened in order to ensure user trust in these transactions.

This particular problem should be viewed from two angles.

First, there is the angle of the electronic transaction itself. For this, one needs to analyze how legal requirements can be formulated that need to ensure that such payments are trustworthily executed. For this, one will have to analyze the requirements set by specific legislation relating to electronic transactions, such as legislation concerning e-commerce. In order to ensure that electronic information is truthful and trustworthy, one can also establish its authenticity and integrity, which will

[21] Article 8 (3) Data Protection Directive.

be important to assess the legal value of said information. This analysis will be performed under this chapter.

Second, one also needs to assess the technology that is used in completing such transactions. As the creation of the personas for this project has already indicated, there are numerous people who generally have a sense of mistrust towards new technologies. In order to ensure that they remain up to speed with ongoing technological evolutions and are thus not excluded from daily societal activities, one will have to demonstrate the trustworthiness of such technologies. With regards to electronic transactions, one can discern a sense of mistrust towards technologies that allow for wireless transactions, thus not requiring physical contact. More specifically, one can think of the use of RFID and NFC. However, also if a transaction does involve physical contact – such as when introducing a bankcard into an ATM – trustworthiness of the transaction will need to be ensured. The rising phenomenon of so-called 'skimmer' devices[22], for instance, raises questions with regards to such transactions with physical contact. The specific problem of assessing the trustworthiness of the technology used in transactions will be analyzed under chapter 4.6 (Technology requirements) of this deliverable

As indicated, this chapter will focus on the legal concerns relating to the electronic transaction itself. First, existing legal provisions regarding such electronic payment transactions will be analyzed in order to formulate the legal requirements for these transactions. Second, it will be analyzed how the trustworthiness of electronic information can be assessed.

4.4.1 Electronic payment transactions

While electronic payment transactions may seem like a straightforward information society evolution of the age-old concept of goods-for-cash, there are a number of specific legal instruments dealing with different aspects of this concept.

First, electronic payment transactions can be understood as an integral part of electronic commerce, also addressed as e-commerce. Within the European Union, e-commerce is generally regulated by the Directive on electronic commerce[23]. This directive is aimed at the services of the information society, which may be interpreted as

> *…any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.*[24]

First, the directive lists a number of information requirements. The service provider is required to make available information relating to his name, geographic address of establishment, contact details, registration number, authorization where such is required for the activity performed, possible professional titles or institutional affiliation and VAT number.[25] Access to this information has to be direct, easy and permanent. Note also the provisions on commercial communications that are aimed at

[22] A skimmer device is usually found at public ATM machines. It involves putting a small card reader over the ATM's card slot, which can copy the information of the card's magnetic strip when introduced into the device. A false keyboard overlaid on the real ATM's keyboard or a camera aimed at the keyboard can register the card's PIN code when inputted by the user. This combination of a copy of the magnetic strip and the PIN code is sufficient to copy and fraudulently use the credit or debit card. As these devices are made to resemble the real ATM, many users are unaware of this activity. In 2009, the Dutch Society of Banks reported estimated damages due to skimming of up to €36 million in The Netherlands alone, a 16% rise compared to 2008. *nvb.nl/index.php?p=514298&return=16963*.

[23] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ* L 178 of 17 July 2000, 1-16 (E-Commerce Directive).

[24] Article 1 (2) Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, *OJ* L 24 of 21 July 1998, 37 *et seq*.

[25] Article 5 (1) Directive 2000/31/EC.

protecting the consumer against false or misleading advertisements and unsolicited commercial communications, better known as spam.[26]

With regards to electronic contracts, the directive requires that Member States need to ensure the legal validity and effectiveness of electronic contracts. Here and in addition to the previous general information requirements, the service provider is required to provide information regarding the technical steps involved in concluding the electronic contract, whether or not that contract will be filed by the services provider and how it can be accessed, the technical means for identifying and correcting input errors prior to the placing of the order and the languages offered for the conclusion of the contract.[27] Also relevant codes of conduct, contract terms and general conditions need to be made available.[28]

In placing the order through technological means, an electronic receipt of the order has to be issued, which is – together with the order itself – deemed to have been received when made accessible to the party to whom it is addressed.[29] The user needs to be given the means to identify and correct input errors before placing the order.[30]

Interestingly, the EU already addressed this issue earlier with the Directive on the protection of consumers in respect of distance contracts.[31] These are contracts that were concluded between consumers and supplier under organized distance sales.[32] Note, however, that article 3 of this directive explicitly states its non-appliance to sales using automatic vending machines. Also here, duties of information and confirmation are imposed onto the seller.[33] The consumer is granted a seven working days period to withdraw from the contract.[34] Note that this directive forms on of the key components of the European Member States' national legal framework on consumer protection.

These two directives can provide a general framework in which electronic contracts for the supply of goods and services can be concluded. The information and confirmation requirements listed here can be used as a general means to inform the consumer about the seller and the nature of the transaction.

Req. F1: In electronic transactions, the service provider is required to inform the consumer about information relating to his name, geographic address of establishment, contact details, registration number, authorization where such is required for the activity performed, possible professional titles or institutional affiliation and VAT number. An electronic receipt of the order received must be issued to the consumer.

Req. F2: In electronic transactions, the service provider is required to provide information regarding the technical steps involved in concluding the electronic contract, whether or not that contract will be filed by the services provider and how it can be accessed, the technical means for identifying and correcting input errors prior to the placing of the order and the languages offered for the conclusion of the contract, including relevant codes of conduct, contract terms and general conditions.

[26] Articles 6 to 8 Directive 2000/31/EC.
[27] Article 10 (1) Directive 2000/31/EC.
[28] Article 10 (2) and (3) Directive 2000/31/EC.
[29] Article 11 (1) Directive 2000/31/EC.
[30] Article 10 (2) Directive 2000/31/EC.
[31] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *OJ* L 144 of 4 June 1997, 19-27.
[32] Article 2 (1) Directive 97/7/EC.
[33] Articles 4 and 5 Directive 97/7/EC.
[34] Article 6 Directive 97/7/EC.

While the directives on e-commerce and distant contracts can provide certain general information requirements for the conclusion of electronic contracts, they do not provide specific provisions relating to electronic payments. As the scenario states that the uTRUSTit device will be used to perform the actual electronic payment, such indicates that this device grants the authorization to, for instance, the vending machine to subtract the due amount from the buyer's account balance.

This raises questions with regards to what is referred to as e-money. Within the EU, the E-Money Directive provides a general framework in which the Member States have to find the ground rules for their national implementations with regards to this topic.[35] E-money is defined as

> *…electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […], and which is accepted by a natural or legal person other than the electronic money issuer".*[36]

Payment transactions are defined as every

> *…act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.*[37]

While e-money cannot be considered to be actual money, it must be defined as being a claim on the bank that has created it [VAN DE VELDE 2008].[38] In principle, if the monetary value would be stored on the device, such would make the uTRUSTit devices application a payment service, thus making the provider of this service a payment institution.[39] This, however, would subject the provider of this service to the strict conditions for being granted the authorization to act as a payment institution within the EU.

However, article 3 (j) of Directive 2007/64/EC holds that these provisions are not applicable to

> *…services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services.*

As it is the scope of the uTRUSTit project to augment trust in these wireless mobile payments, the uTRUSTit application providing for NFC payments could be considered as being such technical service. As a result, the application will have to act as an intermediary, never taking possession of any funds to be transferred. The application needs to be limited to mainly aiding in trust and privacy protection and in providing for data and entity authentication.

> **Req. F3: The application allowing the use of the uTRUSTit device for NFC payments must explicitly state that it is a service provided by a**

[35] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *OJ* L 267 of 10 October 2009, 7-17.

[36] Article 2 (2) Directive 2009/110/EC.

[37] Article 4 (5) Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, *OJ* L 319 of 5 December 2007, 1-36.

[38] Also newer systems using peer-to-peer networks instead of physical cards – such as Bitcoin – could be argued to fall under the scope of the E-Money Directive. It should be noted, however, that the application of this directive to such systems is still subject to debate [JACOBS 2011].

[39] Article 4 (3) and (4) Directive 2007/64/EC.

technical service provider that is aimed at only supporting payment services, trust and privacy protection services and data and entity authentication. No funds to be transferred may be taken into possession at any time.

Other legislation is aimed at regulating the electronic transfer of funds, for instance the Belgian Act of 17 July 2002.[40] This act defines an instrument for the electronic transfer of funds as each means that makes it possible to realize certain actions partly or totally via an electronic way, including the transfer of funds, withdrawals and deposits of cash, access at a distance to an account and charging and discharging of a chargeable instrument.[41] Payments through mobile phones could be understood as payments using a chargeable instrument [VAN DE VELDE 2008].[42] The issuer of an instrument for the electronic transfer of funds is each person who, in his commercial activity, puts an instrument for the electronic transfer of funds at the disposal of another person.[43]

This Act imposes very strict information duties on the issuer and holds clear and strict provisions on his duties and liabilities. Also here, it will therefore be necessary to argue that the provider of the uTRUSTit mobile NFC payments application is a mere intermediary and stores no information, therefore not falling under the scope of the act. Note, however, that divergent national legislations could lead to different interpretations of these concepts.

4.4.2 Trustworthiness of electronic information

Another issue with regards to electronic transactions is the trustworthiness of the electronic information that is conveyed to the buyer. While the previously discussed legislation – such as the E-Commerce Directive – imposes certain information duties on the seller, there are no direct guarantees that this information is correct. This concern was also present in the personas developed for the uTRUSTit project. How can one be sure that the information given by a computer is truthful?

This concern relates to the trustworthiness of electronic information. Establishing the trustworthiness of electronic information is also important to assess the legal evidential value of that information. In general, one can refer to the use of electronic signatures and other techniques to establish the authenticity and integrity of electronic information.

Historically, many legal systems have given preference to written evidence, preferably with a handwritten signature.[44] As it is clear that such handwritten signature cannot be used in an electronic context, one will have to find alternatives. The EU has therefore chosen to implement electronic signatures, stating that a signature in electronic form may not be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.[45] The EU also foresees in an advanced electronic signature, in which a combination of a hashing technique and asymmetric encryption needs to ensure that the signed electronic document was not altered since the moment of signing and to establish authorship of the signature. An even more advanced electronic signature, the qualified electronic signature, adds the use of qualified certificates issued by a qualified certificate service provider that guarantees the identity of the signatory. Such qualified electronic signature must be awarded the same legal value as a handwritten signature.[46]

[40] Act of 17 July 2002 on the transactions executed using instruments for the electronic transfer of funds, *Belgian State Gazette* 17 August 2002.
[41] Article 2, 1° Act of 17 July 2002.
[42] Article 2, 2° Act of 17 July 2002.
[43] Article 2, 3° Act of 17 July 2002.
[44] Note that a handwritten signature is generally understood as the classical signature written using a pen – or similar device – on paper – or similar information carrier. This excludes all use of electronic means.
[45] Article 5 (2) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ* L 13 of 19 January 2000, 12-20.
[46] Article 5 (1) Directive 1999/93/EC.

While the electronic signature has been implemented by all EU Member States and has been accorded reasonable legal value, it may not be the most ideal instrument in establishing authorship of a document and whether the document has been altered, also known as the integrity of the document [DEKEYSER 2006]. For one, the electronic signature relies on contextual information to establish authorship, as the signature itself is a mere code. Also, the electronic signature only provides for integrity at the level of the bitstream, not at the level of the document itself. While a single change in a bit of a file could thus damage its integrity, the actual document contained in the file may not be altered at all.

One could therefore recommend establishing means to assess the authenticity and the integrity of electronic information, which should provide for the trustworthiness of the electronic document. An example is the invoice sent by electronic means, for which a directive has established that it must be accepted by Member States if the authenticity of the origin and the integrity of the content are guaranteed.[47] A 2010 amendment to this provision adds definitions[48]:

> *'Authenticity of the origin' means the assurance of the identity of the supplier or the issuer of the invoice.*
>
> *'Integrity of the content' means that the content required according to this Directive has not been altered.*

Any taxable person is free to determine his means of choice to guarantee authenticity, integrity and legibility of his invoices. Business controls that create a reliable audit trail between invoice and supplied goods or services are recommended. Electronic signatures and Electronic Data Interchange (EDI) is allowed as well. While originally the electronic signature and EDI were the only accepted means to guarantee authenticity and integrity, the EU has now decided to give the taxable person free choice, while giving preference to the use of audit trails.

Audit trails provide a complete log of all transactions pertaining to specific information performed by users or systems. They can be used to trace the origins and whereabouts of information and can as such provide proof of the authenticity of a document and of the document's integrity. With relation to electronic payments transactions, audit trails would be able to guarantee that the author of certain information is truly who he claims to be – for instance, that the author is a bank and not a fraudster posing as a bank – and that the information he transmits has not been altered – which may occur if someone intercepts the data.

> **Req. F4: In order to establish the trustworthiness of electronic information relating to electronic payment transactions, the uTRUSTit mobile NFC payment application is required to guarantee the authenticity and the integrity of the information. The preferred method for providing authenticity and integrity is the use of audit trails, while in secondary order electronic signatures and EDI may be used.**

4.5 Security and access management requirements

Both the Smart Home and the Smart Office scenario displayed a clear need for security and access management, including the possibility for remote access control. This access management ranges from a household's or office's doors or a medicine cabinet to media centers, wireless networks or cloud storage access management. Regardless of whether or not a certain individual person has

[47] Article 233 Directive 2006/112/EC of the Council of 28 November 2006 on the common system of value added tax, *OJ* L 347 of 11 December 2006, 1-118.

[48] Article 1 (22) Directive 2010/45/EU of the Council of 13 July 2010 amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing, *OJ* L 189 of 22 July 2010, 1-8.

indicated that security is important to him or her, adequate security features are imperative for any trustworthy product or service when dealing with the number of interconnections and subsequent potential security risks posed by the IoT. Also from a legal point of view, security has become the subject of specific legal provisions, mainly with regards to the storage of personal data for the processing thereof. Specific requirements looking at security and access management from a legal perspective are therefore needed.

Two key components can be distinguished here. First, one will need to assess the confidentiality component. This component concerns security and access management in its purest form, namely deciding who can enter a certain room or building and who can access certain systems, networks and data. Second, one will need to assess the security of the access management system. What technical and organizational measures are required to guarantee that no unauthorized access is granted?

4.5.1 Confidentiality requirements

The most important component of security and access management is to maintain confidentiality. In essence, this means ensuring that only authorized users are able to gain access to specific facilities, such as a house, computer systems and networks or data. While such access control may seem like a purely technical or organizational issue, the concept of confidentiality has also been included in certain legislation. The most important legal provisions relating to confidentiality can be found in the Data Protection Directive.

From article 16 of the Data Protection Directive follows that only authorized persons should be granted access to the personal data stored for processing. Also, from a combined reading with the proportionality principle, one can deduct that the persons granted access to personal data for their processing under the authority of the data controller – including the processor – should limit their processing to what is instructed to them by the controller or by law [VAN ALSENOY 2011]. This implies a double restriction. First, it needs to be decided who needs to be granted access to the personal data for his processing duties. Second, when authorized to access data, one still needs to be limited to processing only the personal data strictly instructed to be processed by the data controller or by law.

While article 16 of the Data Protection Directive is aimed at ensuring the confidentiality of the processing of personal data, it provides a general sense of the basic requirements that could apply to all access management systems. Not only is it important to clearly delineate who can be granted access to certain facilities, it should also be specified how far these access rights go. For instance in the Smart Office scenario it may be necessary to grant a visitor access to the company's wireless network, while limiting that access to Internet use only and thus not allowing this user access to the company's internal network data.

Also, as already can be deducted from previous analyses, the Smart Home and Smart Office solutions developed in the scenarios display a number of cases in which personal data are processed, notably the Smart Home health monitoring system. For the personal data processed there, the provisions of the Data Protection Directive relating to confidentiality and security are of capital importance. In the case of the health monitoring system, for instance, it was found that health data relating to the data subject would be processed. As health data is considered as a special category of personal data under the Data Protection Directive, more specific and strict rules will apply. In relation to data confidentiality, in particular, this means that in principle only the healthcare provider involved in treating or taking care of the patient should be granted access to the data. For the case of the medicine cabinet developed within the Smart Home scenario, the health data should in principle only be made available to the prescribing physician, the pharmacist and the personal healthcare worker.

In general, the data controller would be required to make an inventory of the different types of personal data that will be processed. Subsequently, he needs to divide the persons acting under his

authority into different groups relating to the specific information necessary for them to perform the processing to which they were instructed. These different groups can subsequently be granted access to the personal data they need. The idea of implementing different levels of access and different groups of users can prove valuable in all types of access management and should thus not be limited to the context of confidentiality for personal data processing.

One can therefore distinguish four stages of granting access [VAN ALSENOY 2007].

First, users need to be registered by the access controller in order to assign them their specific credentials that will be used in providing them access to certain facilities. This will ensure that all users within the access management system are known and given specific access rights.

Second, the user will need to identify himself. This will include the user procuring the identifier to which they agreed upon, which can be his real name, a user name or an identification number.

Third, the user is authenticated. Here, it is verified whether the claim made by the user in stating his identifier was correct. This is the most critical step in the process, as it needs to be verified whether the user is truly who he claims to be or whether he is a fraudster. Here, one can ask him for specific evidence to back his claim, for instance by providing something only the real user can know – such as a password – something only the real user owns – such as an identification card – or something only the real user can be – as in biometric credentials.

Last, the user is authorized. This means that he has been granted access in accordance with the credentials issued to him.

These findings can be summarized in the following requirements.

> **Req. G1: In the processing of personal data, the data controller is required to restrict access to this personal data to the persons that need such access for the processing they perform under his authority. Such access need to comply with the proportionality principle, meaning that no user may be awarded access to more data than strictly required for his processing tasks.**
>
> **Req. G2: In order to achieve such proportional access control, the data controller is required to provide for differentiated access levels for different user groups. This should be combined with an access procedure that includes registration, identification, authentication and authorization.**
>
> **Req.G5: While previous requirements only apply in the context of the processing of personal data, adherence thereto in other cases of access management is strongly recommended as they provide valuable minimal requirements.**

4.5.2 Security requirements

Apart from deciding who is authorized to access certain facilities and how far that access goes, one will also have to adopt appropriate technical and organizational measures to enforce that access control. Within the context of the processing of personal data, article 17 (1) of the Data Protection Directive holds that the data controller needs to take

> *…appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access* […] *and against all other unlawful forms of processing.*

The current state of the art, the costs of implementation, the nature of the data and the nature of the risks are taken into account when judging whether the measures taken were appropriate. This wording does, however, indicate that the obligation on the data controller is merely an obligation of means – as he promises to perform to the best of his ability – and not an obligation of result – where he

is kept to achieve a certain result [VAN ALSENOY 2007]. The data controller does, however, have the duty to ensure that his security policy remains up to date with the ever-evolving standards in security.

With regards to that state of the art, one may notice a few important points that are not directly addressed by the Data Protection Directive, but which should be taken into account in adequate security policies.

First, it should be noted that the European Commission has indicated to

> *…examine the modalities for the introduction in the general legal framework of a general personal data breach notification, including the addressees of such notifications and the criteria for triggering the obligation to notify.*[49]

This development has already received support from the Article 29 Working Party [WORKING PARTY 184]. Such general duty of notification of data breaches is aimed at ensuring that data subjects whose personal data may be affected by the data breach are timely informed of this breach and can take appropriate measures to protect their data, such as blocking their credit card when the card number was made public in a data breach. While this is not aimed at preventing data breaches due to unauthorized access, adequate handling of such breach should be included in security policies.[50]

Second, the state of the art concerning data security should include strong encryption. In order to avoid the principles contained in the Data Protection Directive and subsequent national implementations to become quickly outdated due to rapid technological advancements, it was decided to maintain a level of technological neutrality. As a result, the need for cryptography was not specifically addressed, although it should by current standards of security be considered as a staple in security policies. The use of cryptography should therefore clearly be addressed in a security policy.[51]

Last, implementing adequate security measures should also keep user-friendliness in mind. As indicated in the development of the personas, not all users are willing to be subjected to security policies that require too elaborate procedures. In order to prevent users from refraining from using systems or applications with perceived difficult security procedures or in order to prevent users from simply disabling security features, one will have to ensure that adequate security requires minimal user effort and can run mainly on the background without requiring active user input.

Article 17 (2) of the Data Protection Directive holds that also the processor must be chosen to provide sufficient security guarantees. It is the data controller who must ensure compliance with the technical and organizational measures chosen. A written contract or legal act must bind the data controller and the processor, ensuring that the processor will only act on instructions of the data controller and the obligations relating to the technical and organizational measures to be taken also rest on the processor. Such contract between data controller and processor could also serve as a means to clearly indicate their respective roles and liabilities in the processing of personal data.

The Data Protection Directive also allows for the Member States to adopt additional measures relating to data security. For one, the Belgian Data Protection Act holds in its article 16, §2 that the data controller must keep the data up to date and remove inaccurate, incomplete or irrelevant data, that he must ensure data confidentiality, that he must inform the persons acting under his authority about the provisions of the act and its implementing decrees and that he must assure that the programs used for the automatic processing of personal data are in accordance with the statements made in the notification to the national supervisory authority and that no unlawful use is made thereof.

---

[49] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 4 November 2010, "A comprehensive approach on personal data protection in the European Union", *COM(2010) 609*, 7.

[50] The need for timely notification was stressed clearly in the recent Sony hacks [STUART 2011].

[51] Recent hacks have, however, indicated that encryption is still not always used as a security measure [GOODWINS 2011].

Note that the Belgian national supervisory authority has also advised to adopt a system for audit trails.[52] By logging and tracing all activities, one can later find who accessed particular facilities – including rooms, computer systems and data – and what activities where performed after gaining such access. However, as such extensive logging is a form of personal data processing in itself, one will need to take suitable security precautions when setting up such system for audit trails.

Again, as the principles explicated here are aimed at ensuring data security in the processing of personal data, they do not directly apply to general access management systems. However, as the uTRUSTit scenarios indicate a few instances in which personal data will be processed one will need to provide an adequate level of security for this data. Also, given the importance of these personal data security principles within the European legal framework on data protection, one may refer to them as general obligations, which could easily be transposed to other types of security and access management. Note, however, that these obligations should be interpreted as being minimal obligations. One will always have to keep in mind the current state of the art in data security.

Req. G3: In the processing of personal data, the data controller is required to adopt appropriate and state of the art technical and organizational measures to ensure data security. Also the processor needs to be bound to such security policy.

Req. G4: Such security policy should include, *inter alia*, actions to be taken in case of data breach, the use of cryptography to protect data and audit trails to log and trace data access and use. These security policies also need to take into account user-friendliness and should require minimal user effort.

Req. G5: While previous requirements only apply in the context of the processing of personal data, adherence thereto in other cases of security and access management is strongly recommended as they provide valuable minimal requirements.

4.6 Technology requirements

As indicated in the scenarios developed under Deliverable 2.2 – Definition of User Scenarios – the different IoT solutions envisioned within the uTRUSTit project rely on the use of various technologies. The specific technologies listed here include Radio-Frequency Identification (RFID), Global Positioning System (GPS), Near Field Communication (NFC), Bluetooth and Wi-Fi. As already indicated in chapter 4.2.9 – Radio-frequency identification – of Deliverable 7.1 – Legal Requirements for Trust in the IoT – the use of technologies such as RFID may pose certain privacy concerns. As a result, the use of these technologies will have to be analyzed from a legal point of view in order to develop specific legal requirements to which this use will have to correspond.

The need for such specific legal requirements for the use of these technologies can be deducted from the analysis of the personas developed under Deliverable 2.1 – Personas. As certain users may have a general sense of mistrust towards new technologies, one will have to assure these users that the use of these technologies is bound to specific requirements and that its use can therefore be considered as trustworthy. Such trust building will be necessary to ensure that these users are not excluded from daily societal activities due to their refraining from adapting to technological evolutions.

For the purposes of developing these requirements, the focus will lie on the specific technologies listed in the scenarios. The goal, however, is to develop the requirements in a more technology neutral manner, so as to allow for application thereof to other technologies not specifically mentioned within the Smart Home or Smart Office scenario. As briefly indicated under chapter 4.4 – Electronic payments

[52] *privacycommission.be/en/static/pdf/referenciemaatregelen-vs-01.pdf.*

requirements – of this deliverable, potential risks of data breaches and fraud are not limited to the use of wireless technologies. Also ATMs that require physical contact between the system and the user's bankcard, for instance, could be exposed to risks such as skimming.

4.6.1 General privacy concerns

The use of RFID technology was already analyzed under chapter 4.2.9 – Radio-frequency identification – of Deliverable 7.1 – Legal Requirements for Trust in the IoT. In this analysis, it was found that RFID is considered as an important building block for the IoT, but that certain privacy concerns, for instance regarding the transparency of the use of this technology, remain [UTRUSTIT 2011b]. Several bodies – including the European Commission, the EDPS and the Article 29 Working Party – have already issued opinions on the use of RFID, where the general consensus is that no specific legal framework for the use of this technology is required. As a result, the use of RFID is considered to be covered by the Data Protection Directive, thus requiring such use to be subjected to the general principles concerning data protection.

In particular, the Article 29 Working Party brought two issues to the forefront: awareness and deactivation [Working Party 105; UTRUSTIT 2011b]. First, the data subject needs to be made aware of the presence of RFID tags around him. As RFID tags can made to be very small, they can easily be hidden – for instance in the seams of clothes – thus not being noticeable to the data subject. By clearly indicating the presence of RFID tags, data subjects may become more confident towards this technology. Second, the purpose of the RFID tags should be limited and they should be deactivated when their purpose has been attained. In the case of a security tag, for instance, the tag on an item should be disabled after its purchase. As a result, the data subject should be made aware of the activity of the RFID tags in his surroundings and should know whether they are – or can be – deactivated.

In order to ensure that future RFID applications are compliant with general privacy regulations and the specific provisions of the legal framework on data protection, a Privacy Impact Assessment (PIA) was proposed. Such assessment would analyze the potential privacy and data protection concerns to be made with regards to proposed future RFID applications. Taking into account the results of this assessment, producers of RFID applications should thus ensure that their product is fully compliant before it enters the market. Such proactively ensuring privacy compliance is part of what is generally referred to as privacy by design.

Privacy by design aims to achieve privacy compliance of technology from its creation on, not by *ex post* assessment and subsequent modifications. In this vision, privacy compliance should become the default mode of operation and not an afterthought. While Privacy-Enhancing Technologies (PETs) were originally seen as potential tools to augment privacy implementation, privacy by design is now recommended as a means to maintain full functionality in an organization while at the same time promoting privacy.[53] In general, one can distinguish seven foundational principles for privacy by design [CAVOUKIAN 2009].

First, privacy by design should be characterized by its proactive nature. It is not aimed at *ex post* reactions against privacy infringements, but at taking actions before such invasion occurs.

Second, privacy by design aims to have full privacy protection as an automatic given in any IT system or business practice. One should not have to opt-in into better privacy settings as these should be the default option.

Third, privacy should be included in the basic design of the system or business from the very beginning, not an extra feature that is added later. By embedding privacy, it becomes a core component.

[53] In 2010, the 32nd International Conference of Data Protection and Privacy Commissioners adopted a resolution supporting privacy by design: *privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf.*

Fourth, privacy by design aims to maintain full functionality. It aims at demonstrating that no trade-offs need to be made between, for instance, privacy and security. Both can be implemented by making the right choices in the parties' interests.

Fifth, privacy should be maintained throughout the full lifecycle of the data collected.

Sixth, visibility and transparency should be promoted for all stakeholders to see and verify that all stated objectives are followed.

Seventh, privacy should be aimed at the interests of the data subject, thus including privacy defaults, notices and user-friendly options in all systems and businesses. User-centricity should be maintained.

These findings can be summarized in the following requirements.

Req. H1: Regardless of the technology used, the data subject should be made fully aware of the presence of the technology and of its activities and the possibility for deactivation.

Req. H2: A Privacy Impact Assessment should be used to assess privacy compliance of technologies and applications from their development phase on. Such should ensure *ex ante* compliance with privacy and data protection provisions.

Req. H3: Other privacy by design principles should be used as a guideline for embedding privacy compliance from the very start, thus avoiding later modifications aimed at achieving compliance.

More in general, one should also refer to the general data protection requirements – as formulated in chapter 4.1 – General data protection requirements of this deliverable – and, more specifically, the security and access management requirements – as formulated in chapter 4.5 – Security and access management requirements of this deliverable. As the wireless technologies mentioned in the scenarios may transfer personal data during certain activities, such transfer will need to be adequately secured. The general data protection requirements and the security and access management requirements should provide for the minimal obligations to attain adequate security coverage.

The need for adequate security can easily be demonstrated by the example of the Belgian Mobib card [VANDEZANDE 2010]. This RFID-equipped smart card is used as an electronic ticket, or e-ticket, for access to the Brussels public transport network. The card holds information on the user's full name, date of birth, address and his last three itineraries. As it turns out, this data is not adequately secured, enabling anyone with a suitable RFID-reader to read and collect passengers' personal data from a distance. Although the Belgian national supervisory authority, the Privacy Commission, recommended that customer data and e-ticket data should be kept separate and that the information on these cards should be secured, no additional security measures have been implemented yet [VANDEZANDE 2011]. Also the Dutch public transport smart card has been hacked, exposing many passengers to a potential data breach of their personal data [SCHELLEVIS 2011]. As more services are implementing such RFID-based systems, or systems based on similar technologies, the need for trustworthy connections and data storage is becoming ever more urgent.

4.6.2 Geolocation applications

The technologies mentioned in the Smart Home and Smart Office scenario are not only intended to be used as a means for data transfer. They can also be used for geolocation and tracking purposes. In the scenario for the Trusted Smart Home health monitoring system, for instance, the uTRUSTit device can be used to locate a person requiring medical surveillance and to track his movements.

The use of geolocation services, with specific relation to smart mobile devices, was the subject of a recent Article 29 Working Party opinion [WORKING PARTY 185]. In this opinion, the Working Party

remarks how all information – such as health data and financial data – can be linked to a geographic location and that these geolocation services therefore hold great potential impact on their users' privacy. E-ticketing is named as an example where the user's movements can be traced and – as seen in the Mobib example discussed earlier – where this information could be coupled to other personal data of this user. The Working Party describes a number of geolocation technologies, such as base station data, GPS and Wi-Fi.

As mobile devices are closely linked to an individual, they may hold several types of personal data on this user. This may include sensitive data, for instance when tracking the individual's movements to a hospital or religious places. Such tracking is often unnoticed by the user, for instance if an application runs geolocation services in the background without informing the user.

Geolocation data may lead to the identification of a natural person, or may make this person identifiable. Therefore, this data needs to be regarded as personal data. Even when the particular technology used cannot provide an exact identification of the natural person, the obtained geolocation data should still be considered as personal data.[54]

As a result, the provisions of the Data Protection Directive are applicable to the providers of geolocation services. Given the nature of such services, prior informed consent would be the most viable justification ground for the processing of this personal data. Consent should be revocable and should also be regularly renewed, thus limiting the validity of consent in time. The Working Party advises that the user should be made aware when geolocation services are activated, for instance by a visible icon. By default, such services should be switched off. Also granularity is addressed, as the Working Party finds that the user should be given the option to choose how precise his geolocation data is – ranging from State, province and city to street and number, which can also be referred to as "location blurring".

The findings of the Article 29 Working Party's opinion can be formulated into general requirements for geolocation services.

Req. H4: As geolocation data must be viewed as personal data, the processing thereof must comply with the principles of the Data Protection Directive and its national implementations.

Req. H5: Prior informed consent must be obtained for the processing of geolocation data. This consent must be revocable and must be regularly renewed.

Req. H6: Geolocation services must be switched off by default. The user must be made aware of active geolocation services. The user must also be given the option to choose the granularity of his consent. The user must also be given the option to opt-out from databases containing Wi-Fi access points.

4.7 Intellectual property rights requirements

The Trusted Smart Home Entertainment Management application demonstrated potential legal implications with regards to copyright protection. As likely most of the media to be managed, played and possibly shared using this application will still be subjected to copyright protection, one could have to ensure that the Trusted Smart Home Entertainment Management application does not actively allow for copyright infringements.

[54] *The fact that in some cases the owner of the device currently cannot be identified without unreasonable effort, does not stand in the way of the general conclusion that the combination of a MAC address of a WiFi access point with its calculated location, should be treated as personal data.* [WORKING PARTY 185]

Two questions can be raised in this regard. First, could the use of the Trusted Smart Home Entertainment Management application, with regards to managing, playing and sharing media lead to a copyright infringement? Second, can the producer of the Trusted Smart Home Entertainment Management application be held liable if his application is misused by its users for copyright infringements?

4.7.1 Possibility of copyright infringements

In terms of managing and playing media, the Trusted Smart Home Entertainment Management application seems to comply with legitimate use of copyright protected media. The application is mainly used to manage and play media within a single household and for invited friends. If this media was obtained legitimately, the copyright license must have been paid and such use would therefore be allowed. Also temporary reproductions made in part of technological processes – such as loading the media in a system's cache memory – are allowed, if these reproductions are

> *…transient or incidental and an integral and essential part of a technological process*

and are aimed at

> *…a transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made, and which have no independent economic significance.*[55]

Sharing the media, however, may pose a different challenge. While the scenario for the Trusted Smart Home Entertainment Management application seems to indicate that the media is obtained through a trustworthy – and thus presumably legitimate – third party e-payment service and that no media is shared beyond the household, the wishes of the Fredrik persona indicate that he wants to share media data with his friends.

In principle, copyright protection in many States holds a right to make a reproduction of the work for personal use within a household.[56] In many cases, authors are still granted remuneration for such reproduction.[57] In the case of media data sharing beyond a household, the right to a personal copy – as the reproduction for personal use is often referred to as – will be violated. It is also uncertain whether any remuneration to the author was paid in such sharing, unless the data was shared using a medium on which a compulsory copyright license fee was levied.

Therefore, if such media data is shared beyond a single household – for instance, if the media data is transferred from Fredrik's house to a friend's house – without proper compensation to the copyright holders, this sharing would constitute what is widely known as media piracy. While piracy is at times considered as theft, the lack of actual stolen property dismisses such definition.[58] Piracy should therefore only be considered as an infringement to the exclusive rights of the copyright holder.

The right to a personal copy, however, has also been the center of certain controversy. In Dutch copyright law, for instance, it is generally accepted that the right to a personal copy does not discriminate on the origins of the work copied for personal use. As a result, downloading copyright protected works without paying compensation to the author – generally understood as illegal downloading – could still be regarded as the exercise of the right to a personal copy, if the downloaded copy is only put to personal use and thus not shared with third parties[59].[60] Such reasoning is rather

[55] Article 5 (1) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ* L 167 of 22 June 2001, 10-19.

[56] For instance: Article 22, §1, 5° of the Belgian Copyright Act: Act of 30 June 1994 on authors' rights and related rights, *Belgian State Gazette* 27 July 1994.

[57] By compulsory licenses on media carriers, see article 55 Belgian Copyright Act.

[58] Dowling *v* United States, 473 U.S. 207 (1985).

[59] While close friends could be argued to be part of the household, such is a decision subject to the court's discretion [WERKERS 2006].

unique as, for instance, the Belgian Copyright Act does explicitly state that the copyright protected work copied for personal use needs to be made public in a legitimate manner.[61] Although it can be argued that this provision needs to be interpreted as referring to the author's initial divulgence of his work – and thus not including a potentially illegally uploaded copy of the work after said divulgence – this reasoning is not shared by the bodies responsible for enforcing copyright within the Belgian territory.

As a result, one can conclude that making a copyright protected work public without proper licensing from the holder of the copyright – such as in transferring it to a friend – will always be an infringement to that copyright. Illegally obtaining such works – as through illegal downloading – can only in highly limited cases be considered as falling under the scope of the personal copy and will therefore in most cases also be seen as an infringement to copyright.

4.7.2 Producer's liability for copyright infringements

As it is clear that the Trusted Smart Home Entertainment Management application could be misused by its users for copyright infringements, one will have to assess whether the producer of such application can be held liable for the illegitimate practices to which the application was put to use by its users.

The most well known example in case law to be found here is the Napster case, in which the producers of the Napster application were found guilty in illegally distributing copyright protected works.[62] An important element in this case was that Napster had a large degree of control on and personal involvement in its network, thus being aware of the copyright infringements by its users and also having the possibility to interfere with such possible infringements.

Other examples, such as Grokster, had a lesser degree of control and only provided the means to their users, who used these means for copyright infringements. As a result, Grokster was initially only held liable as contributory to the acts of their users. The US Supreme Court, however, found that Grokster's behavior – in promoting itself as an alternative to Napster and gaining revenue from what it knew to be illegal activities by its users – was sufficient to be considered as inducing copyright infringements by its users.[63]

Also KaZaA was found to be liable, by an Australian court, for the infringements committed by its users as its producers should have known that their network was used by users to commit copyright infringements and that they authorized such infringements by not acting against them.[64] The Dutch Supreme Court, however, found that file sharing as a technique is no direct infringement of copyright and that KaZaA did not have the personal capacity to control its network in such way as to prevent its users from committing copyright infringements.[65] As a result, KaZaA was not held liable for the actions of its users.

Another example is the so-called torrent websites that host BitTorrent files that contain the metadata necessary to download the associated data from different users. The operators of the most well known example of such torrent website, The Pirate Bay, were found guilty of accessory to copyright infringements.[66] Even though the website itself did not host any illegal content, it was found to have assisted illegal file sharing in such way that it constituted criminal liability for the operators of the website.

---

[60] Article 16b and 16c of the Act of 23 September 1912 on the new rules regarding author's rights, *Dutch State Gazette* 1912, 308. Case law and parliamentary discussions confirm this reasoning: Gerechtshof 's-Gravenhage, ACI c.s. *v* Stichting De Thuiskopie & SONT, 15 November 2010, *LJN BO3982*; Kamerstukken Tweede Kamer 28482, nr. 5, 2002-2003, 33.

[61] Article 22, §1 of the Belgian Copyright Act.

[62] A&M Records, Inc. *v* Napster, Inc., 239 F.3d 1004 (2001).

[63] MGM Studios, Inc. *v* Grokster, Ltd. 545 U.S. 913 (2005).

[64] Universal Music Australia Pty Ltd *v* Sharman License Holdings Ltd., FCA 1242 (2005).

[65] Dutch Supreme Court C02/186HR BUMA/STEMRA *v* Kazaa BV, 19 December 2003, *LJN AN7253*.

[66] Svea Court of Appeal B 4041-09 Sony BMG Music Entertainment AB *et al. v* Fredrik Neij *et al.*, 26 November 2010.

These cases serve as an example that the producers of an application that could be used by its users for illegal file sharing may be held liable – fully or accessory – if it is found that the producers were aware of such illegitimate use and failed to act against it. One could therefore advise the producers of such applications to assess what measures could be taken against misuse by their users as such misuse could result in liability of the producers.

One can also refer to the liability exemption of intermediary service providers, analyzed under chapter 5.2.2 (Liability of service providers) of D7.1 (Legal Requirements for Trust in the IoT). As discussed, the Internet service providers that provide to their users access to the Internet will, if they comply with the provisions regarding the liability exemption, not be held liable if their services fall under the scope of mere conduit, caching or hosting [UTRUSTIT 2011b]. This has, however, not halted copyright enforcement bodies to seek action against Internet service providers.[67]

From this overview, it becomes clear that the Trusted Smart Home Entertainment Management application could be misused by its users for what constitutes illegal sharing of media data – namely sharing without proper license and without proper remuneration to the author of the copyright protected work. As the pursuit of such file sharing users is often costly, time consuming and raises questions with regards to the protection of user privacy, many authorities seek to address the providers of the services through which the file sharing is performed or even of the Internet service providers that provided Internet access to such users. Given the many differences in national legislation and the divergent outcomes of existing case law, it would be advised that the producers of the Trusted Smart Home Entertainment Management applications ensure that they cannot be held liable for potential misuse of these applications by their users. One important element here is that of intent: the producers of the applications need to clearly demonstrate that it was not their intent to have their applications misused for illegal file sharing. This can be formulated in the following requirement:

> **Req. I1: Producers of the Trusted Smart Home Entertainment Management applications are required to assess whether their applications can be misused by users for illegal file sharing. Where technically feasible, measures are to be taken in order to prevent such misuse as producers of applications and service providers may in certain cases be held liable for copyright infringements by their users.**

[67] Notably in the case of the Belgian Society of Authors, Composers and Publishers against Internet service provider Scarlet, it was sought that Scarlet would be ordered to continuously and actively monitor its traffic in order to track piracy. After a number of national cases, a prejudicial question was transferred to the ECJ. Recently, the Advocate-General M. Pedro Cruz Villalón has concluded that a national measure requiring all Internet service providers to actively and continuously monitor all of their traffic would infract Community law. The Court's final decision is currently pending. ECJ C‑70/10 Scarlet Extended SA *v* Société belge des auteurs compositeurs et éditeurs (Sabam), opinion of the Advocate-General of 14 April 2011.

5. Consolidation of Legal Requirements

In the previous analyses, a number of specific legal requirements for the Smart Home and Smart Office scenario were developed. These requirements will be consolidated and completed here.

A. BASIC DATA PROTECTION REQUIREMENTS

Req. A1

IoT actors identified as data controllers must be aware of the precise definitions of national data protection legislation applicable to the processing under their control. Collaboration with the competent national Data Protection Authority will ensure a correct understanding of the specific national implementation of the definitions of the applicable notions.

Req. A2

The data subject's free, informed, specific and unambiguous consent must be obtained for legitimate processing of personal data. While such consent is only one of the possible justification grounds for legitimate personal data processing, it will in most cases be the only viable justification ground for personal data processing with relation to the IoT.

→ *Further on consent, see Requirements D*

Req. A3

Fair and lawful processing of personal data must demonstrate legality or transparency.

Req. A4

The purposes of the processing of personal data must be clearly indicated in advance.

Req. A5

The processing of personal data may only include relevant and non-excessive data, in relation to the specified purposes. Data must be collected for a specified, explicit and legitimate purpose and may not be further processed in a way incompatible with those purposes.

Duration of data storage must be limited and stored data must be destructed once the purpose for which that data was collected has been attained.

Req. A6

Data minimization can also be achieved by employing methods for anonymization or pseudonymization of personal data. Here, data unlinkability should be kept in mind as linkability could lead to the identification of a particular data subject.

Req. A7

The data controller must ensure sufficient information of the data subject.

Req. A8

The data controller must ensure that the data subject can fully enforce his right of access, his right to correction and his right to object.

Req. A9

Special notice must be paid to the special categories of personal data, such as health data. These categories of personal data may only be processed on limited and strict justification grounds.

→ *With regards to health data, see Req. E3*

Req. A10

The data controller must ensure confidentiality and security of the processing of personal data under his control.

→ *Further on confidentiality and security, see Requirements G*

Req. A11

Due notification must be made to the competent national Data Protection Authority (or Authorities), in compliance with national legislation.

Req. A12

Data transfers to third States must comply with applicable legislation.

B. DATA PROTECTION AT HOME

Req. B1

Processing of personal data of family members of the same household must be executed in a personal capacity and strictly for purposes in the personal or household sphere, with restricted publicity of this data. Failure to observe personal capacity, personal or household purposes or to keep data publicity limited will result in the non-applicability of the household exception. As a result, the processing of this personal data must comply fully with all personal data processing requirements.

Req. B2

Also when no personal data is processed or when the household exception applies, any intrusion to the personal sphere of family members – including minor children – will be considered as a violation of their privacy. Prior consent must therefore be granted.

C. DATA PROTECTION AT WORK

Req. C1

As in *Req. A7*, workers must be informed about the data their employer is collecting about them, directly or from other sources, for which processing purposes envisioned or performed with this data currently or in the future. Transparency must also be assured by granting the data subject the right to access to his or her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.

Req. C2

As in *Req. A3,* the processing of workers' personal data must be legitimate. Article 7 of the Data Protection Directive lists the criteria making the processing legitimate.

Req. C3

As in *Req. A5,* the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed. Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker.

Req. C4

Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified.

Req. C5

As in *Req. A10*, the employer must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access.

Req. C6

Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.

Req. C7

As in *Req. A1*, the precise capacity in which one party performs personal data processing on behalf of another party must be clearly established. Employees must be clearly identified as such in order to distinguish them from their employer/data controller and the external processor.

Req. C8

In order to determine their compliance with the means and purposes of a personal data processing, assistive technologies must clearly indicate whether, how and for what period of time logs containing personal data are stored, for what purpose, what data they contain precisely and by whom they can be accessed.

D. CONSENT REQUIREMENTS

Req. D1

Carefully drafted privacy policies and consent forms – for instance in a multi-layered format – must ensure compliance to the requirement of consent and the right to information. Note that such privacy policies and consent forms must be compliant with national data protection legislation. For instance, certain jurisdictions require written consent, while others allow for implicit consent in many cases.

Req. D2

User-friendliness should be the focal point in obtaining the data subject's consent. While unintelligible texts may lead to the data subject not reading a privacy policy or consent form, elaborate procedures to grant consent may result in the data subject refraining from using such service, thus damaging the business of the data controller. A balance between the interests of both parties should therefore be struck.

Req. D3

When dealing with minors, elderly and/or persons with a mental illness, the data controller is advised to seek consent from both the data subject and its statutory or legal guardians. The general legal capacity of the data subject determines its capacity to consent.

Req. D4

Informed consent must be given freely. In order to determine whether the data subject's consent was given freely, one must analyze the external pressure exercised on his decision. Positive persuasion cannot invalidate his freely given consent, while negative coercion will invalidate his consent as it could not have been given freely.

Req. D5

Consent should be limited in time and should be renewed for continuously ongoing processing of personal data. Consent should also be revocable.

E. HEALTH MONITORING

Req. E1

In using technologies that could potentially lead to a continuous collecting and processing of personal data, one must assess the proportionality of such collecting and processing. Mostly, the purpose for which the technology is used and for which the data is processed does not necessarily require continuous data processing. Therefore, one must select the least intrusive yet suitable means that lead to minimal data collection and storage.

Req. E2

As consent requires certain negotiability and as consent can be revoked, the health monitoring system must allow for certain adaptability of the system to the specific needs and wishes of the person under medical surveillance. This person must be offered the option to – temporary or

permanently – disable the features that he deems to intrusive, in line with expected amendments to the Data Protection Directive.

Req. E3

When health data is processed as part of the health monitoring system, the data controller must obtain the explicit – or written, where applicable – consent of the legally capable data subject as justification ground for the processing of this special category of personal data. In case of legal incapacity of the data subject, the processing of his health data can only be performed if necessity for the protection of his vital interests can be demonstrated.

F. ELECTRONIC PAYMENT TRANSACTIONS

Req. F1

In electronic transactions, the service provider must inform the consumer about information relating to his name, geographic address of establishment, contact details, registration number, authorization where such is required for the activity performed, possible professional titles or institutional affiliation and VAT number. An electronic receipt of the order received must be issued to the consumer.

Req. F2

In electronic transactions, the service provider must provide information regarding the technical steps involved in concluding the electronic contract, whether or not that contract will be filed by the services provider and how it can be accessed, the technical means for identifying and correcting input errors prior to the placing of the order and the languages offered for the conclusion of the contract, including relevant codes of conduct, contract terms and general conditions.

Req. F3

The application allowing the use of the uTRUSTit device for NFC payments must explicitly state that it is a service provided by a technical service provider that is aimed at only supporting payment services, trust and privacy protection services and data and entity authentication. No funds to be transferred may be taken into possession at any time.

Req. F4

In order to establish the trustworthiness of electronic information relating to electronic payment transactions, the uTRUSTit mobile NFC payment application must guarantee the authenticity and the integrity of the information. The preferred method for providing authenticity and integrity is the use of audit trails, while in secondary order electronic signatures and EDI may be used.

G. CONFIDENTIALITY AND SECURITY

Req. G1

In the processing of personal data, the data controller must restrict access to this personal data to the persons that need such access for the processing they perform under his authority. Such access need to comply with the proportionality principle, meaning that no user may be awarded access to more data than strictly required for his processing tasks.

Req. G2

In order to achieve proportional access control, the data controller must provide for differentiated access levels for different user groups in order to ensure proportionality. This must be combined with an access procedure that includes registration, identification, authentication and authorization.

Req. G3

In the processing of personal data, the data controller must adopt appropriate and state of the art technical and organizational measures to ensure data security. Also the processor must be bound to such security policy.

Req. G4

Such security policy should include, *inter alia*, actions to be taken in case of data breach, the use of cryptography to protect data and audit trails to log and trace data access and use. These security policies should also take into account user-friendliness and should require minimal user effort. When using audit trails, the data controller must define the purposes and scope of this logging and make transparent who can access these logs as audit trails constitute personal data processing.

Req. G5

While previous requirements only apply in the context of the processing of personal data, adherence thereto in other cases of security and access management is strongly recommended as they provide valuable minimal requirements.

H. TECHNOLOGY REQUIREMENTS

Req. H1

Regardless of the technology used, the data subject should be made fully aware of the presence of the technology and of its activities and of the possibility for deactivation.

Req. H2

A Privacy Impact Assessment should be used to assess privacy compliance of technologies and applications from their development phase on. Such should ensure *ex ante* compliance with privacy and data protection provisions.

Req. H3

Other privacy by design principles should be used as a guideline for embedding privacy compliance from the very start, thus avoiding later modifications aimed at achieving compliance.

Req. H4

As geolocation data must be viewed as personal data, the processing thereof must comply with the principles of the Data Protection Directive and its national implementations.

Req. H5

Prior informed consent must be obtained for the processing of geolocation data, as this will mostly be the only viable justification ground for the processing of this data. This consent must be revocable and must be regularly renewed.

Req. H6

Geolocation services should be switched off by default. The user should be made aware of active geolocation services. The user should also be given the option to choose the granularity of his consent. The user should also be given the option to opt-out from databases containing Wi-Fi access points.

I. COPYRIGHT

Req. I1

Producers of the Trusted Smart Home Entertainment Management applications should assess whether their applications can be misused by users for illegal file sharing. Where technically feasible, measures should be taken in order to prevent such misuse as producers of applications and service providers may in certain cases be held liable for copyright infringements by their users.

6. Summary

In this deliverable the general legal requirements derived from the general privacy framework that devices should comply with as a prerequisite for trust and the general liability framework – as conceived under Deliverable 7.1-Legal Requirements for Trust in the IoT – were applied to the Office and Home Scenario developed under Deliverable 2.2-Definition of User Scenarios, as well as to the Personas developed under Deliverable 2.1-Personas.

In order to ensure legal compliance by the prototype to be designed within the uTRUSTit project, the Scenarios and Personas were analyzed to identify a number of key legal issues that needed further assessment. First, the general data protection requirements were completed focusing on the needs for privacy and data protection at home and at work. Second, the issue of informed consent was analyzed with regards to the effectiveness of consent and the capacity to consent. Third, the health monitoring system was analyzed, resulting in legal requirements regarding the adaptability of the system and the processing of health data by such system. Fourth, the use of electronic payments was analyzed from the perspective of electronic payment transactions and the trustworthiness of electronic information. Fifth, security and access management aspects were found to need specific confidentiality and security requirements. Sixth, the use of the technologies of the IoT was analyzed from the point of view of general privacy concerns and the rising use of geolocation applications. Last, the possibility of copyright infringements by the media sharing system was analyzed, also focusing on the potential liability of the producers of such system for copyright infringements by its users.

The research conducted here has resulted in a more concrete list of requirements, reiterating and complementing the general legal requirements formulated under Deliverable 7.1-Legal Requirements for Trust in the IoT. These new requirements can serve as a means to ensure full legal compliance by the uTRUSTit prototype up from its earliest design and development stages.

7. References

7.1 Legislative sources

EU: Founding Treaties

- Charter of Fundamental Rights of the European Union, *OJ* C 83 of 30 March 2010, 389 *et seq*.

EU: Directives

- 2010/45/EU of the Council of 13 July 2010 amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing, *OJ* L 189 of 22 July 2010, 1-8.
- Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *OJ* L 267 of 10 October 2009, 7-17.
- Article 4 (5) Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, *OJ* L 319 of 5 December 2007, 1-36.
- Directive 2006/112/EC of the Council of 28 November 2006 on the common system of value added tax, *OJ* L 347 of 11 December 2006, 1-118.
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ* L 167 of 22 June 2001, 10-19.
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ* L 178 of 17 July 2000, 1-16 (E-Commerce Directive).
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ* L 13 of 19 January 2000, 12-20.
- Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, *OJ* L 24 of 21 July 1998, 37 *et seq.*
- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, *OJ* L 144 of 4 June 1997, 19-27.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , *OJ* L 281 of 23 November 1995, 31-50.

EU: European Commission

- Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 4 November 2010, "A comprehensive approach on personal data protection in the European Union", *COM(2010) 609*, 6.
- Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "Internet of Things — An action plan for Europe", *COM(2009) 278*, 5-6.
- Commission Green Paper of 16 October 1996 on the protection of minors and human dignity in audiovisual and information services, *COM(1996) 483*, 12.

Council of Europe

- Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome, 4 November 1950.

United Nations

- United Nations Convention on the Rights of the Child, 20 November 1989, A/RES/44/25.

Belgium

- Act of 13 June 2005 regarding electronic communications, *Belgian State Gazette* 20 June 2005.
- Act of 17 July 2002 on the transactions executed using instruments for the electronic transfer of funds, *Belgian State Gazette* 17 August 2002.
- Act of 30 June 1994 on authors' rights and related rights, *Belgian State Gazette* 27 July 1994.
- Collective Labour Agreement nr. 81 of 26 April 2002 regarding the protection of the privacy of employees with regards to the monitoring of electronic communications data, *www.nar-cnt.be*.

The Netherlands

- Act of 23 September 1912 on the new rules regarding author's rights, *Dutch State Gazette* 1912, 308.
- Kamerstukken Tweede Kamer 28482, nr. 5, 2002-2003, 33.

7.2 Case law

ECJ

- ECJ C‑70/10 Scarlet Extended SA *v* Société belge des auteurs compositeurs et éditeurs (Sabam), opinion of the Advocate-General of 14 April 2011.
- ECJ C‑73/07 Tietosuojavaltuutettu *v* Satakunnan Markkinapörssi Oy & Satamedia Oy, 2008, §44.
- ECJ C-101/2001 Bodil Lindqvist, 2003, §46-47.

ECHR

- ECHR 62617/00 Copland *v* the United Kingdom, 2007, §§ 41-42.

USA

- MGM Studios, Inc. *v* Grokster, Ltd. 545 U.S. 913 (2005).
- A&M Records, Inc. *v* Napster, Inc., 239 F.3d 1004 (2001).
- Dowling *v* United States, 473 U.S. 207 (1985).

Australia

- Universal Music Australia Pty Ltd *v* Sharman License Holdings Ltd., FCA 1242 (2005).

The Netherlands

- Dutch Supreme Court C02/186HR BUMA/STEMRA *v* Kazaa BV, 19 December 2003, *LJN AN7253*.
- Gerechtshof 's-Gravenhage, ACI c.s. *v* Stichting De Thuiskopie & SONT, 15 November 2010, *LJN BO3982.*

Sweden

- Svea Court of Appeal B 4041-09 Sony BMG Music Entertainment AB *et al. v* Fredrik Neij *et al.*, 26 November 2010.

7.3 Legal literature

- [ALLEN 2011] ALLEN, A., WARDEN, P. (2011). Got an iPhone or 3G iPad? Apple is recording your moves. *radar.oreilly.com*, 20 April 2011.

- [WORKING PARTY 185] ARTICLE 29 WORKING PARTY (2011). Opinion 13/2011 on Geolocation services on smart mobile devices. *WP 185.*
- [WORKING PARTY 184] ARTICLE 29 WORKING PARTY (2011). Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments. *WP 184.*
- [Working Party 105] ARTICLE 29 WORKING PARTY (2005). Working document on data protection issues related to RFID technology. *WP 105.*
- [WORKING PARTY 55] ARTICLE 29 WORKING PARTY (2002). Working document on the surveillance of electronic communications in the workplace. *WP 55*.
- [WORKING PARTY 48] ARTICLE 29 WORKING PARTY (2001). Opinion 8/2001 on the processing of personal data in the employment context. *WP 48.*
- [BESSELINK 2003] BESSELINK, L.F.M. (2003). Voetangels en klemmen: de horizontale werking van burger- en politieke rechten. In: FLINTERMAN, C., VAN GENUGTEN, W. (eds.) (2003). *Niet-Statelijke actoren en de rechten van de mens: gevestigde waarden, nieuwe wegen*. Den Haag: Boom Juridische Uitgevers, 3-18.
- [DEKEYSER 2006] DEKEYSER, H. (2006). Authenticity in bits and bytes. in NEEF, S., VAN DIJCK, J. and KETELAAR, E. (eds.). *Sign Here! Handwriting in the age of New Media*. Amsterdam: Amsterdam University Press, 2006, 76-90.
- [DUMORTIER 2010] DUMORTIER, J. (2010). *ICT-Recht*. Leuven: Acco, 277p.
- [VANWIJNGAERDEN 2008] VANWIJNGAERDEN, J.S. (2008). De werking van grondrechten tussen particulieren, geïllustreerd met voorbeelden. *Jura Falconis*, 44, nr. 2, 217-248.
- [UTRUSTIT 2011b] DUMORTIER, J., VANDEZANDE, N. (eds.*)* (2011). uTRUSTit - D.7.1 Legal Requirements for Trust in the Internet of Things. www.*utrustit.eu*, 75p.
- [GOODWINS 2011] GOODWINS, R. (2011). Sony hacked again in Lulzsec breach. *zdnet.co.uk*, 3 June 2011.
- [ILO 1997] INTERNATIONAL LABOUR OFFICE (1997). Code of *Practice on the Protection of workers' personal data*. Geneva: International Labour Office, 4.
- [JACOBS 2011] JACOBS, E. (2011). Bitcoin: a bit too far? *timelex.eu*, 25 June 2011.
- [KOSTA 2011] KOSTA, E. (2011). *Unravelling consent in European data protection legislation - a prospective study on consent in electronic communications*. Doctoral Thesis Faculty of Law, K.U.Leuven, 364p.
- [UTRUSTIT 2010] SCHULZ, T., ELLENSOHN, L. (eds.) (2010). uTRUSTit - D.2.9 Synchronization Workshop on Taxonomy, Requirements and Scenarios with WP3 and WP4. *www.utrustit.eu*, 13p.
- [UTRUSTIT 2011a] SCHULZ, T., GRAF, C. (eds.) (2011). uTRUSTit - D.2.1 Personas. *www.utrustit.eu*, 20p.
- [UTRUSTIT 2011b] DUMORTIER, J., VANDEZANDE, N. (2011). uTRUSTit - D.7.1 Legal Requirements for Trust in the Internet of Things. *utrustit.eu*, 75p.
- [UTRUSTIT 2011c] SCHULZ, T., FRITSCH, L., *et al.* (eds.) (2011). uTRUSTit - D.2.2 Definition of User Scenarios. *www.utrustit.eu*, 31p.
- [SCHELLEVIS 2011] SCHELLEVIS, J. (2011). OV-chipkaart voor studenten is gekraakt. *tweakers.net*, 16 February 2011.
- [STUART 2011] STUART, K., ARTHUR, C. (2011). PlayStation Network hack: why it took Sony seven days to tell the world. *guardian.co.uk,* 27 April 2011.
- [VAN ALSENOY 2007] VAN ALSENOY, B. (2007). IM3 Interactive Mobile Medical Monitoring - Task HE 2.1.1: Legal requirements analysis. *www.ibbt.be*, 128p.
- [VAN ALSENOY 2011] VAN ALSENOY, B. (ed.) (2011). GINI - D3.1 Legal provisions for deploying INDI services. *www.gini-sa.eu*, 88p.
- [VAN DE VELDE 2008] VAN DE VELDE, J. (2008). NFC Voucher – Deliverable 1.4: Legal framework and requirements. *IBBT*, 85p.
- [VANDEZANDE 2011] VANDEZANDE, N. (2011). Verder omtrent Mobib: begin van rechtszaak en van parlementair debat. *Privacy & Informatie* 2011/3, 166.

- [VANDEZANDE 2010] VANDEZANDE, N. (2010). Aanbeveling Privacycommissie over e-ticketing. *Privacy & Informatie* 2010/4, 205-206.
- [WERKERS 2006] WERKERS, E., GILIO, F. (2006). De complexe verhouding tussen peer-to-peer-netwerken en de exceptie van de privékopie: kan de driestappentest een evenwicht tot stand brengen? *Computerrecht*, 289.